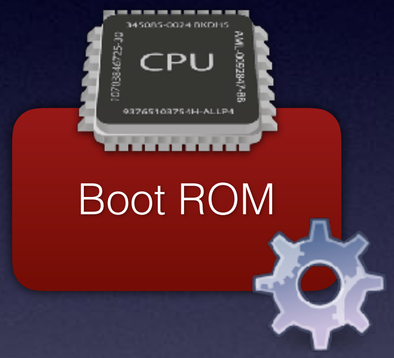
Marrying U-Boot, UEFI and grub

About Me

- Alexander Graf
- KVM and QEMU developer for SUSE
  - Server class PowerPC KVM port
  - Nested SVM
- Founding member of SUSE ARM team

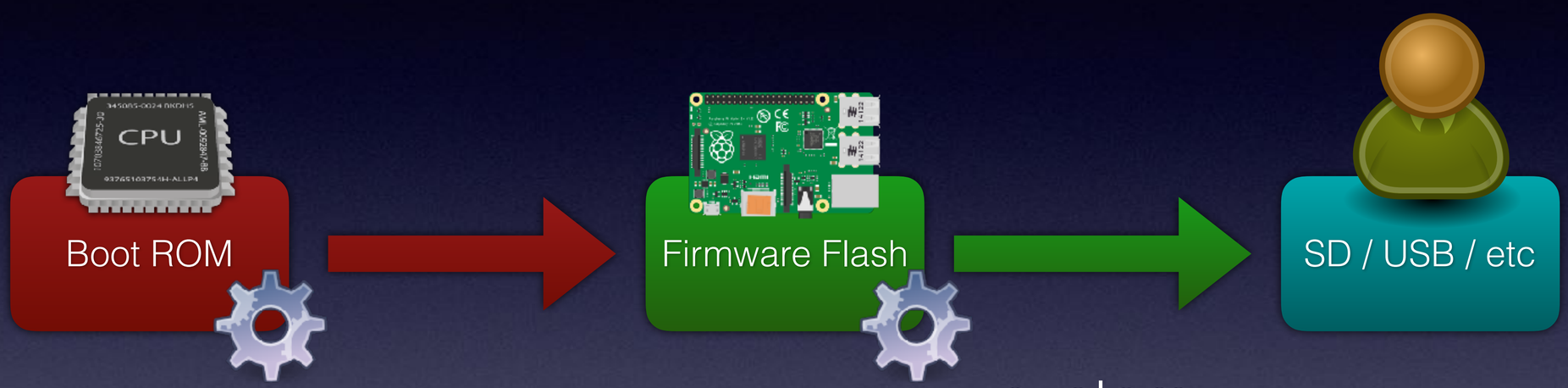
Booting on ARM

Booting on ARM



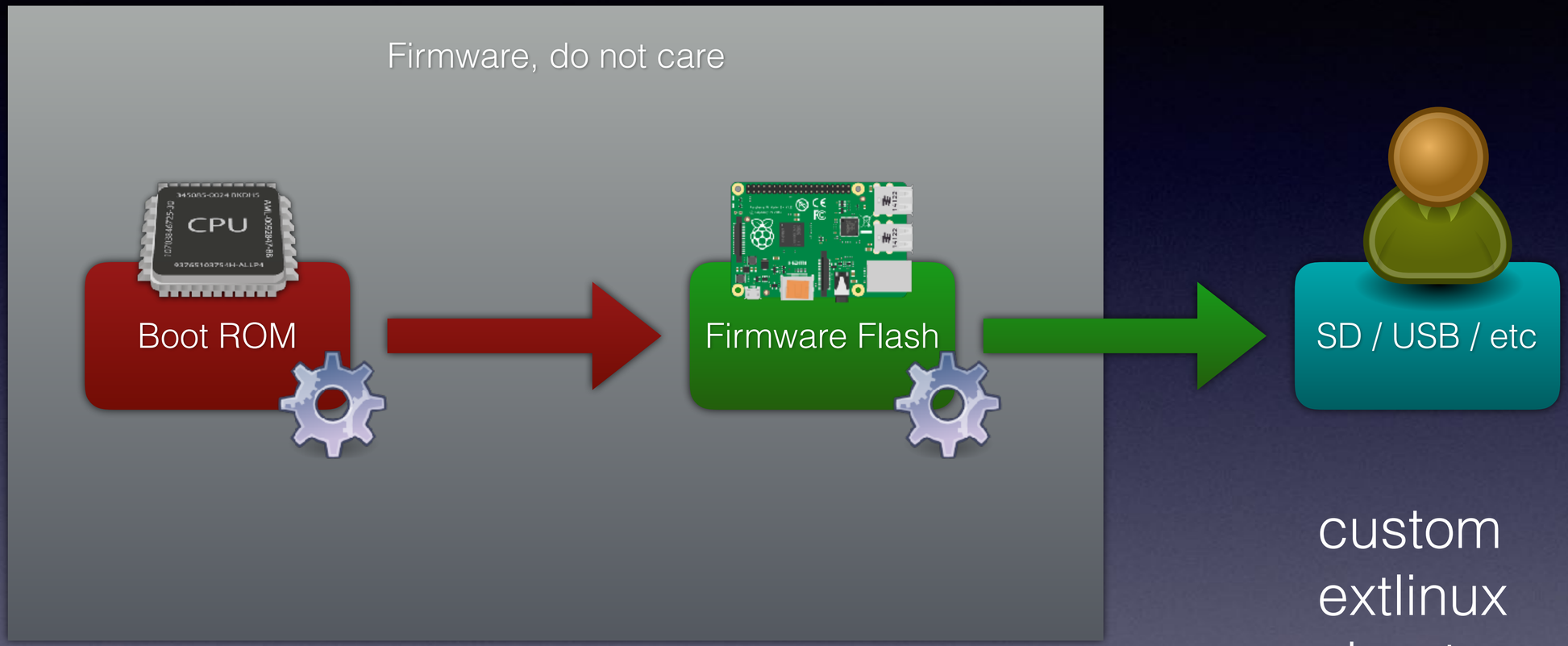
Booting on ARM

Booting on ARM



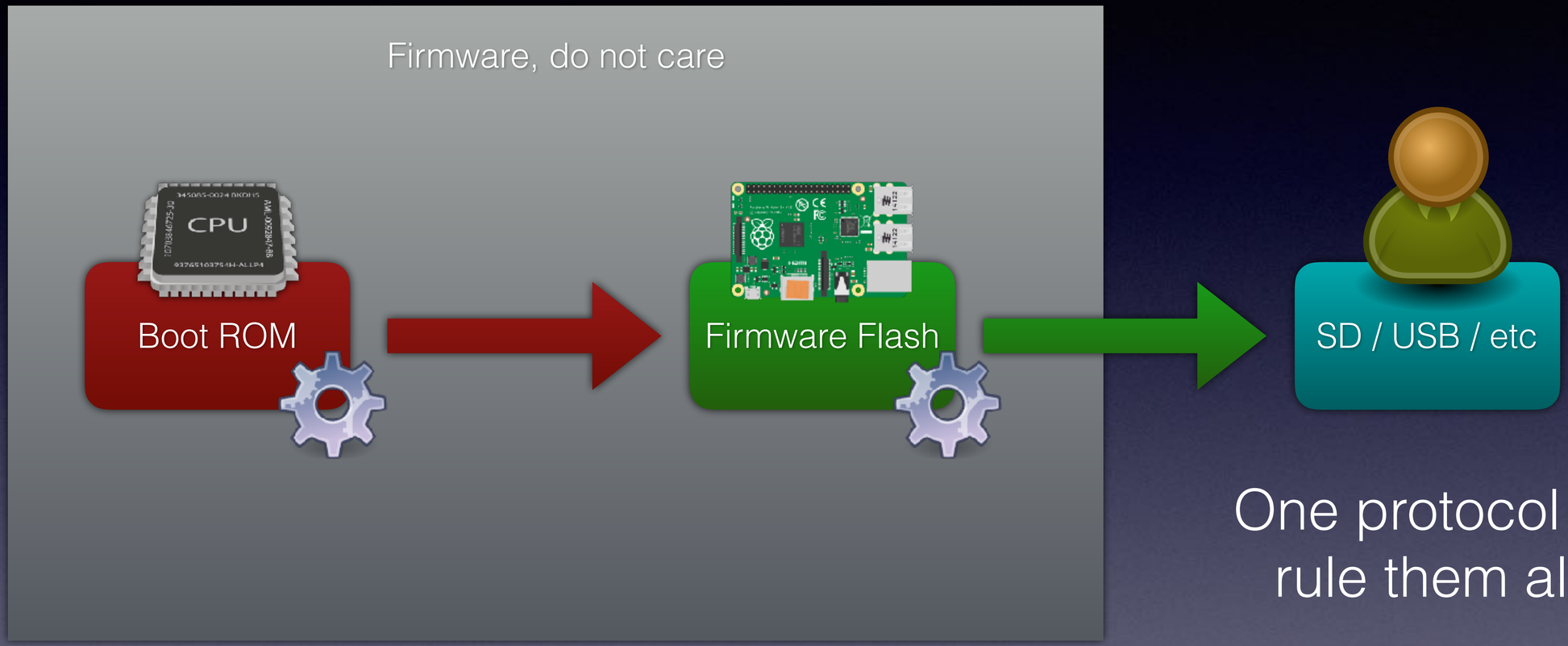
custom
extlinux
vboot
UEFI

Ideal Distro boot flow



custom
extlinux
vboot
UEFI

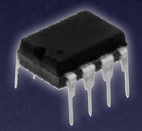
Ideal Distro boot flow



One protocol to rule them all

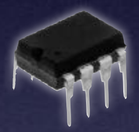
UEFI boot flow

UEFI boot flow

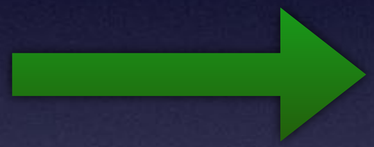


UEFI

UEFI boot flow



UEFI



NVRAM

UEFI boot flow

UEFI

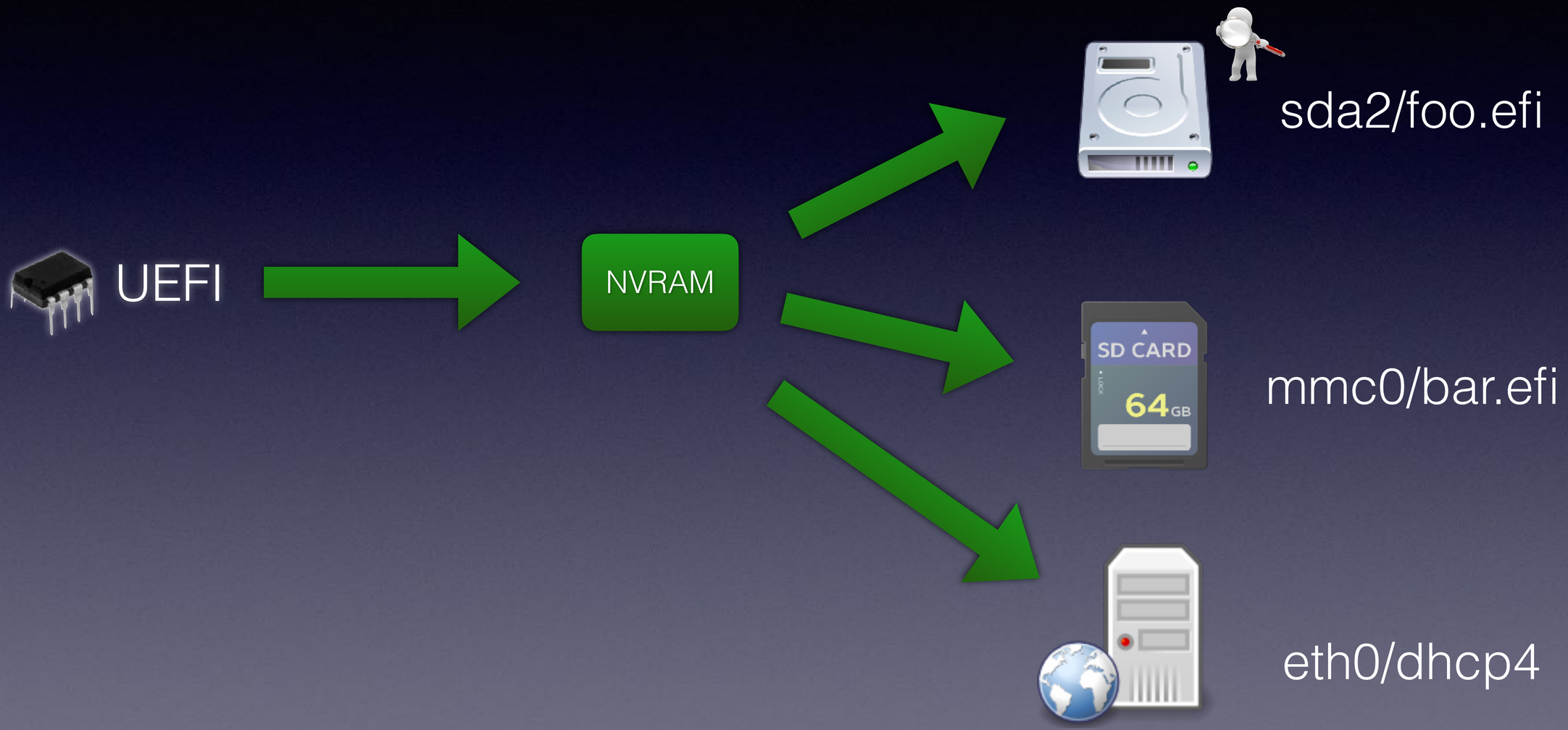
NVRAM

sda2/foo.efi

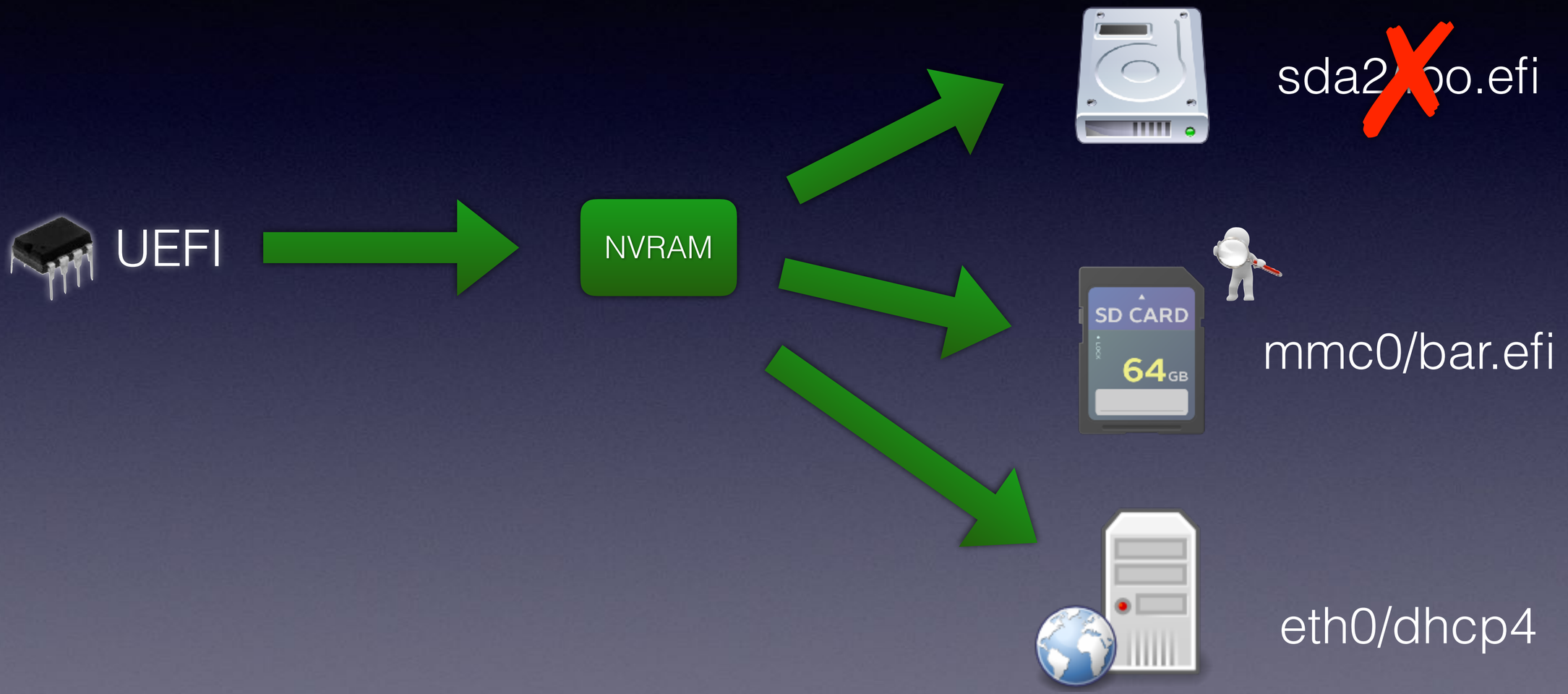
mmc0/bar.efi

eth0/dhcp4

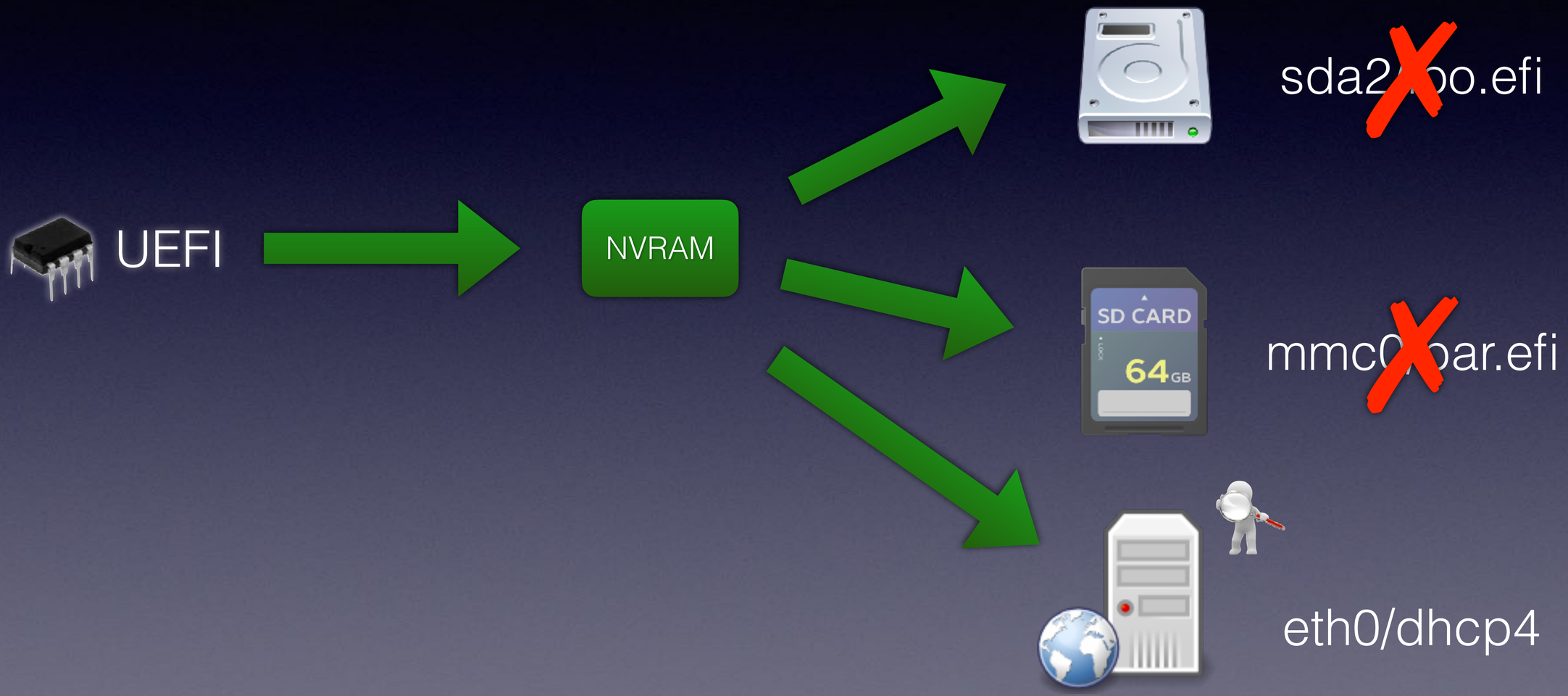
UEFI boot flow



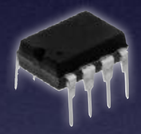
UEFI boot flow



UEFI boot flow



UEFI boot flow



UEFI

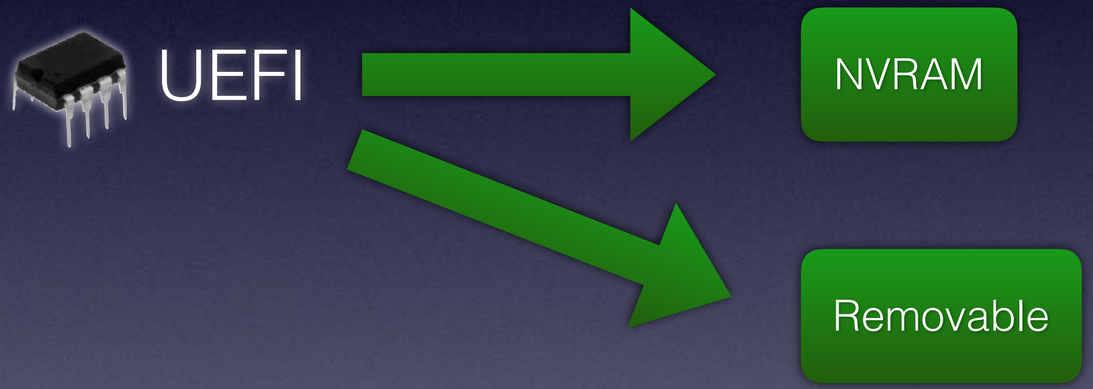
NVRAM

sda2/boo.efi

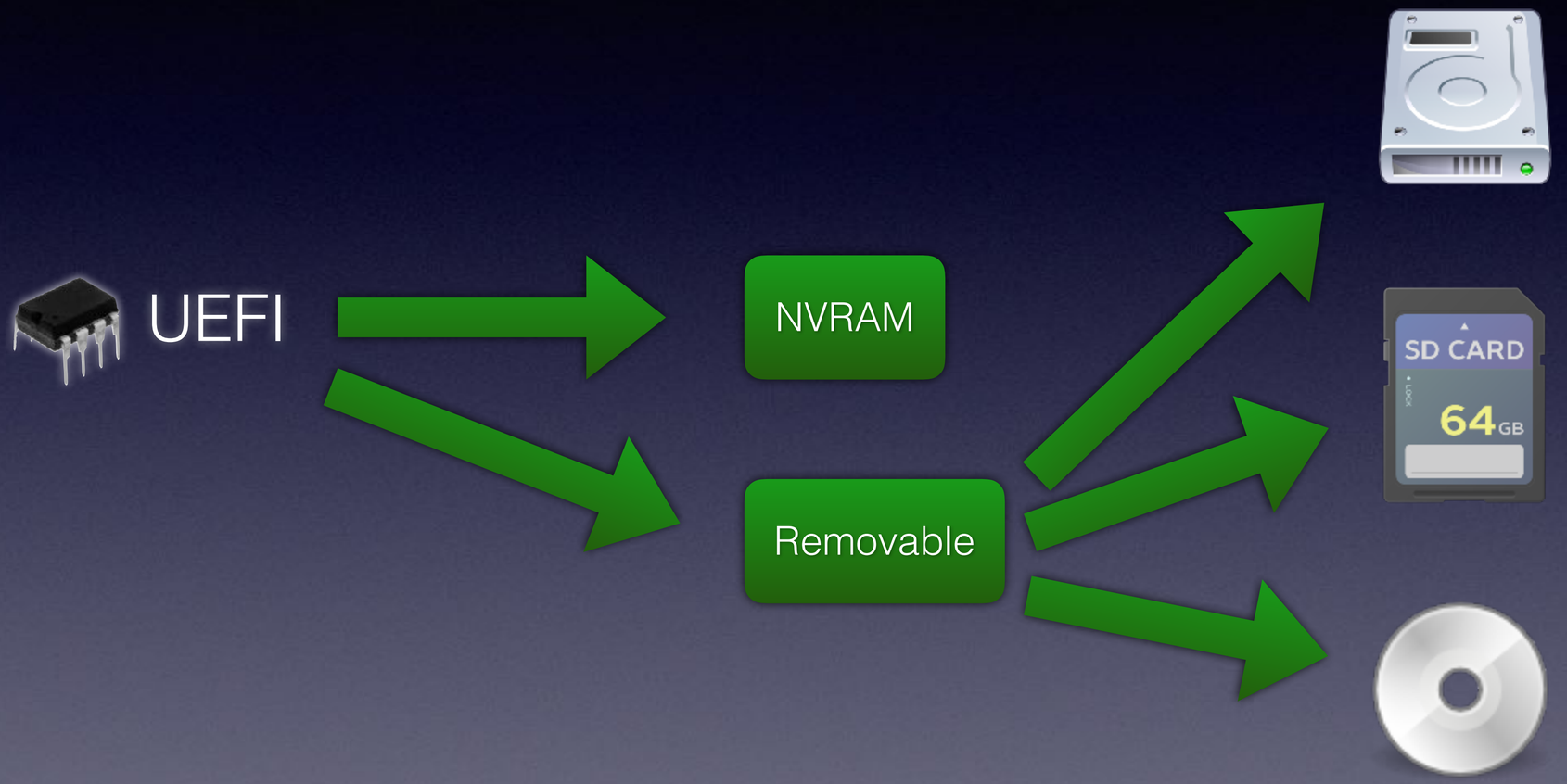
mmc0/boar.efi

eth0/dhcp4

UEFI boot flow



UEFI boot flow

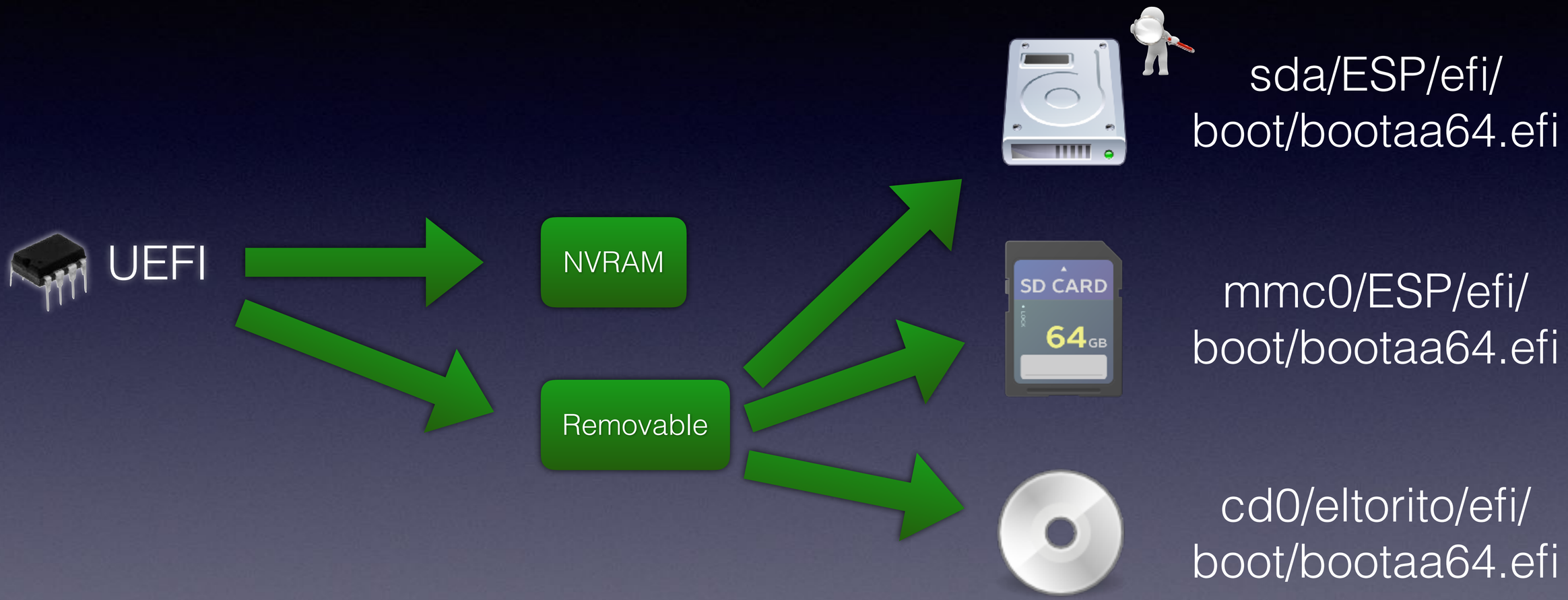


sda/ESP/efi/
boot/bootaa64.efi

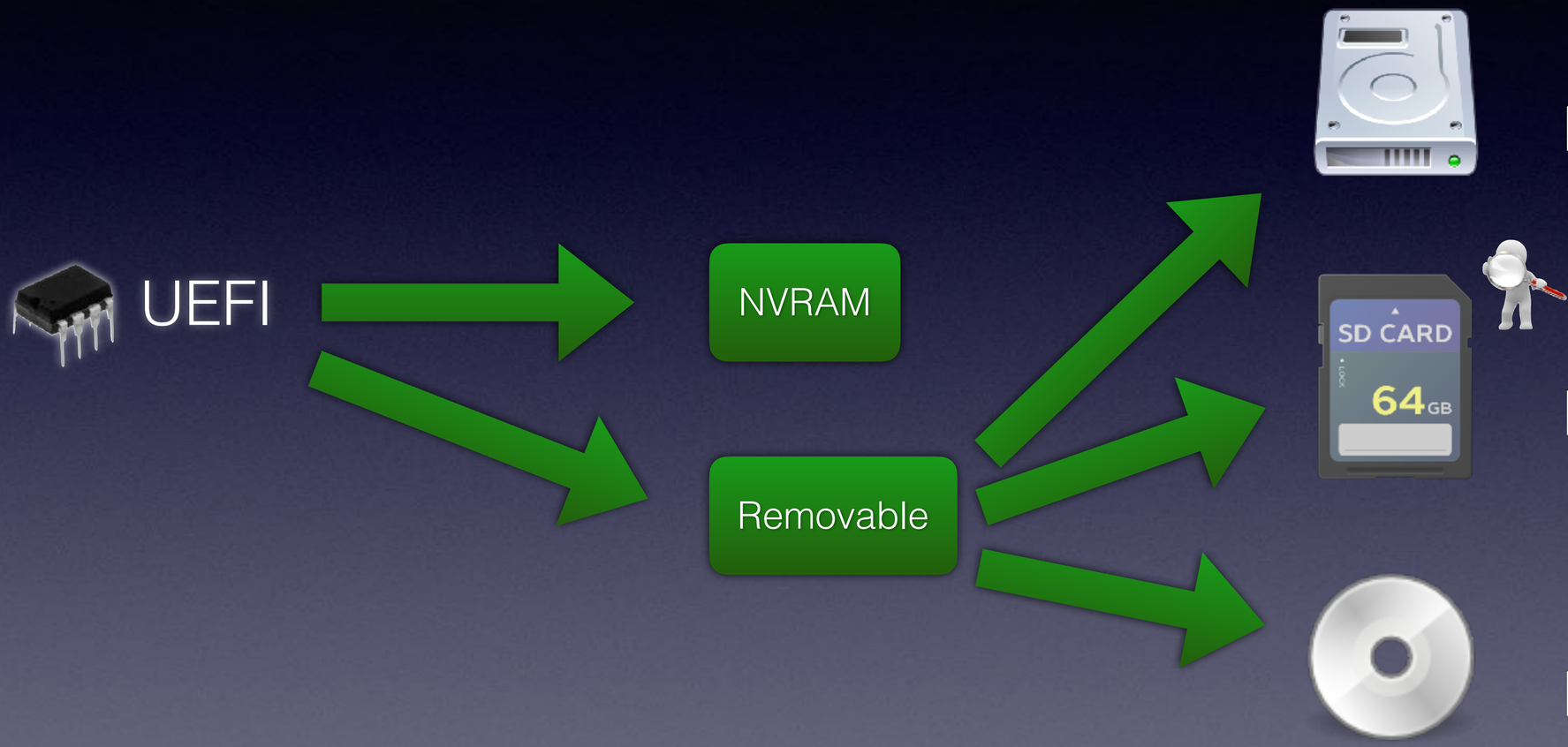
mmc0/ESP/efi/
boot/bootaa64.efi

cd0/eltorito/efi/
boot/bootaa64.efi

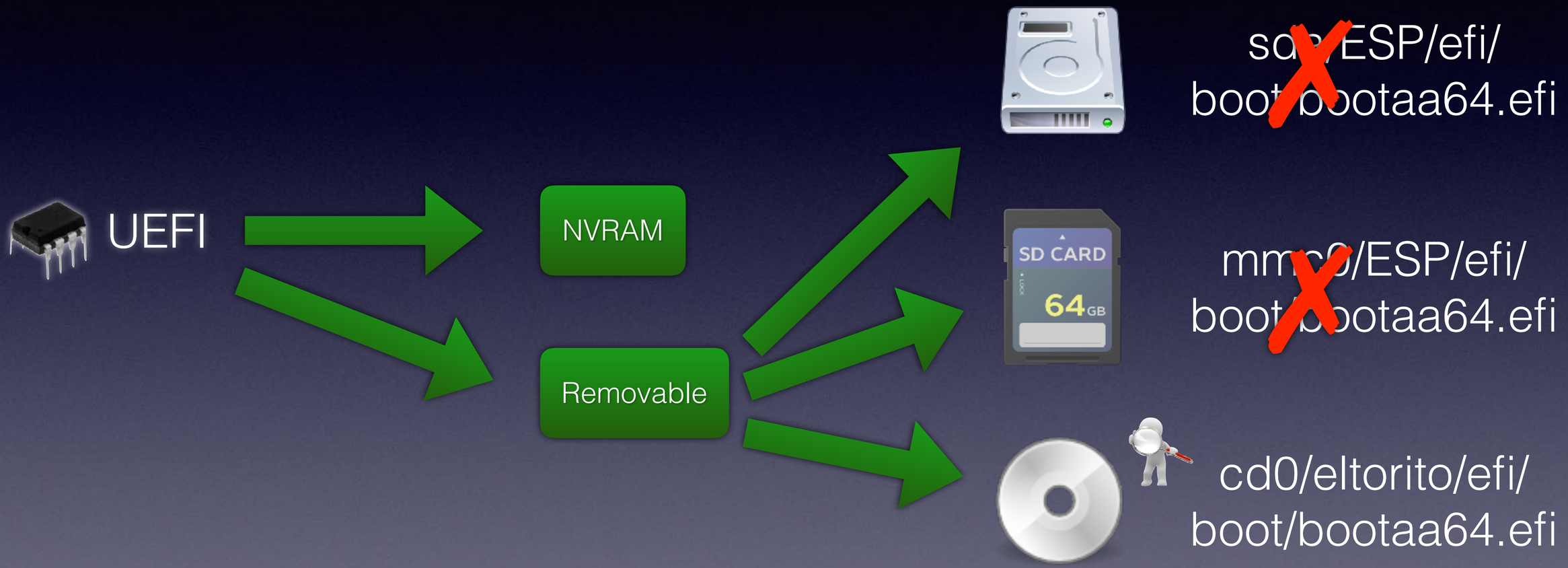
UEFI boot flow



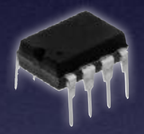
UEFI boot flow



UEFI boot flow



UEFI boot flow



UEFI

NVRAM

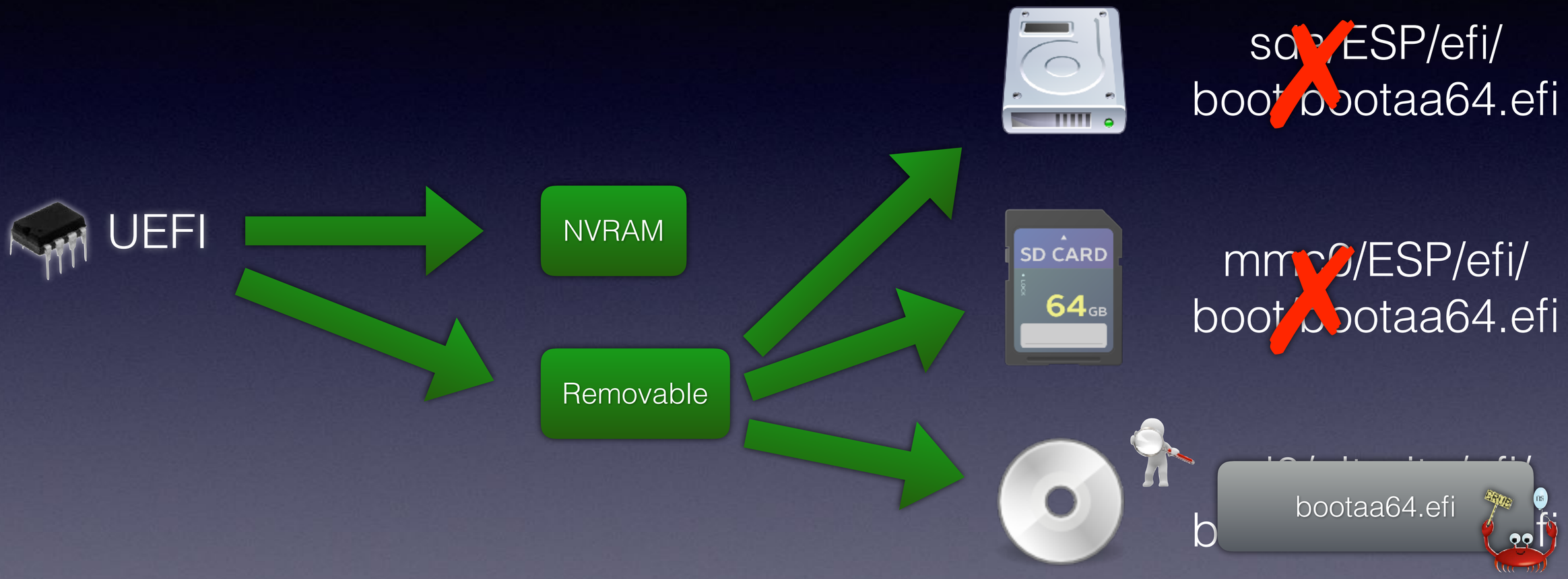
Removable

sd?/ESP/efi/
boot/bootaa64.efi

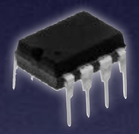
mmc0/ESP/efi/
boot/bootaa64.efi

cd0/eltorito/efi/
boot/bootaa64.efi

UEFI boot flow



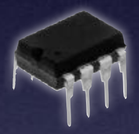
UEFI boot flow



UEFI

bootaa64.efi

UEFI boot flow



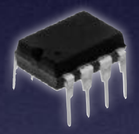
UEFI

bootaa64.efi

EFI Runtime Data

Console
Boot Services
Runtime Services
Tables

UEFI boot flow



UEFI

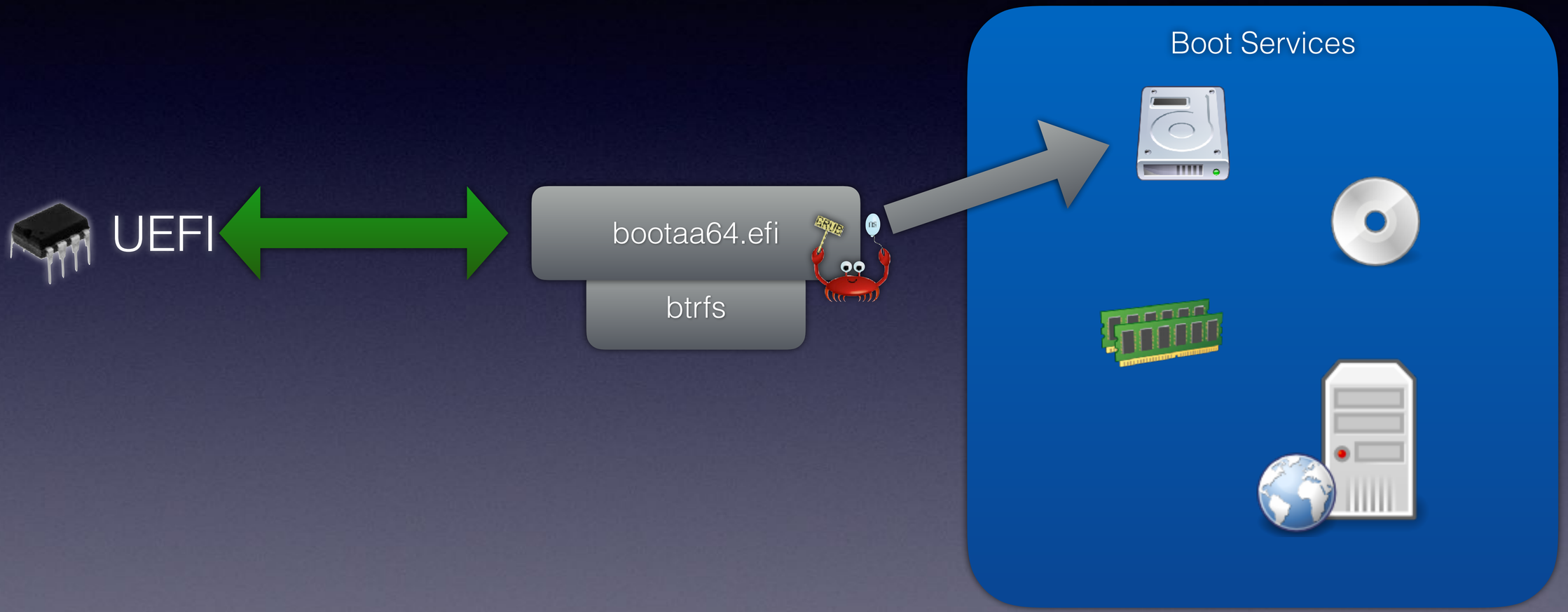
bootaa64.efi

EFI Runtime Data

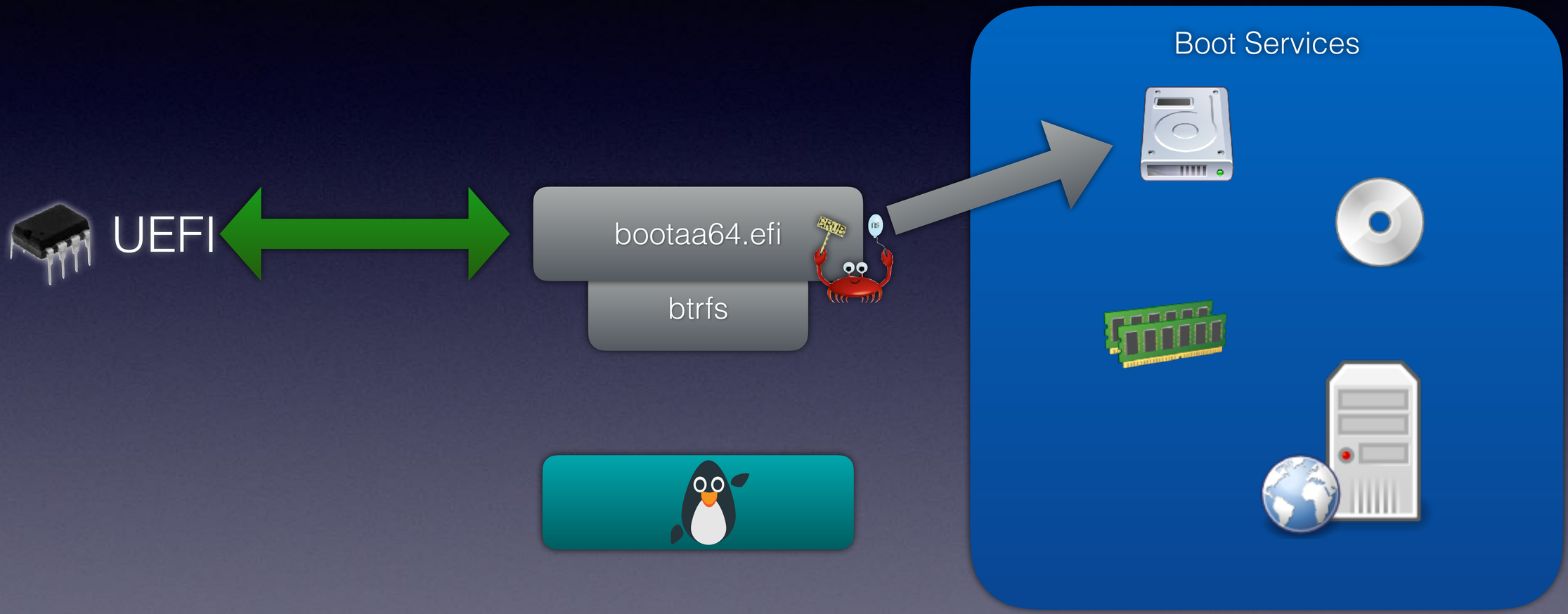
Console
Boot Services
Runtime Services
Tables

UEFI boot flow

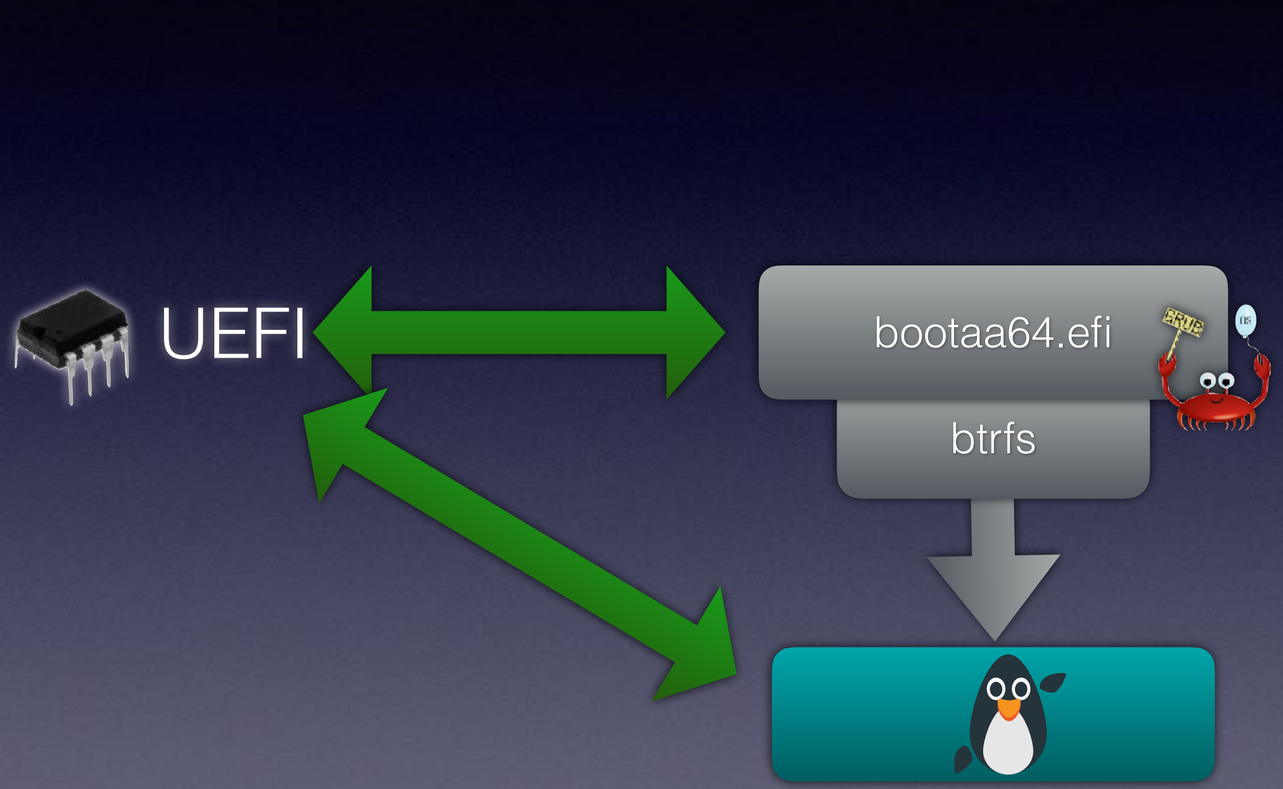
UEFI boot flow



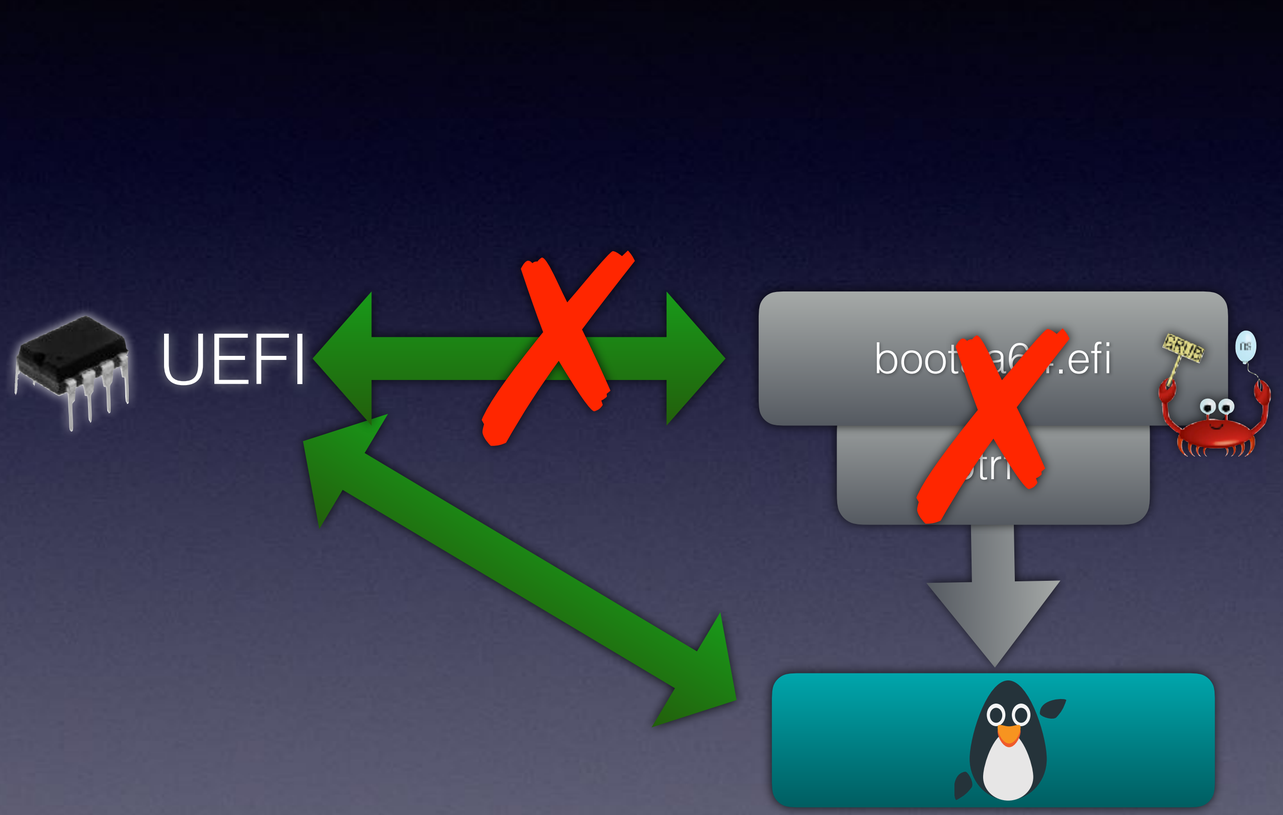
UEFI boot flow



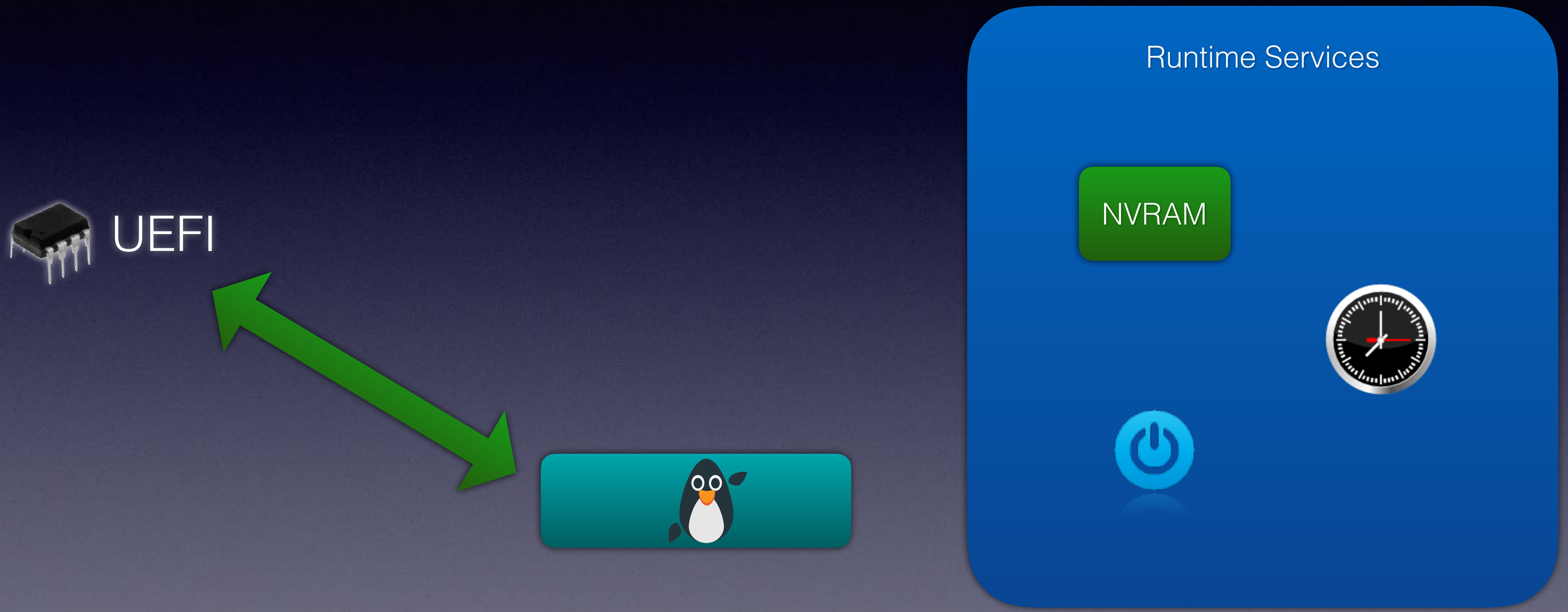
UEFI boot flow



UEFI boot flow



UEFI boot flow



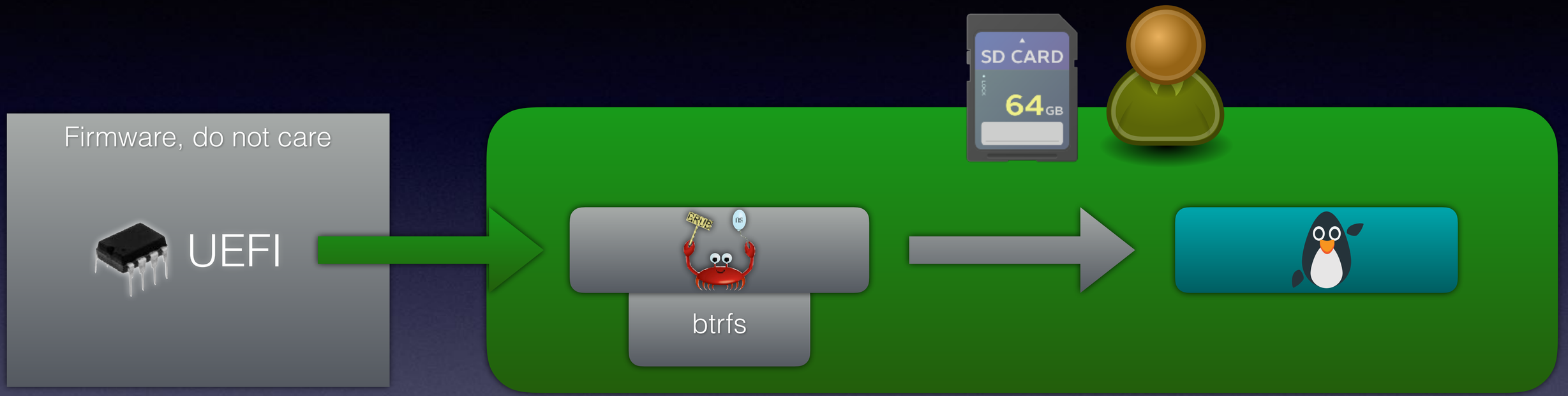
UEFI boot flow advantages

UEFI boot flow advantages

UEFI boot flow advantages

UEFI boot flow advantages

UEFI boot flow advantages



UEFI boot flow advantages

UEFI boot flow advantages

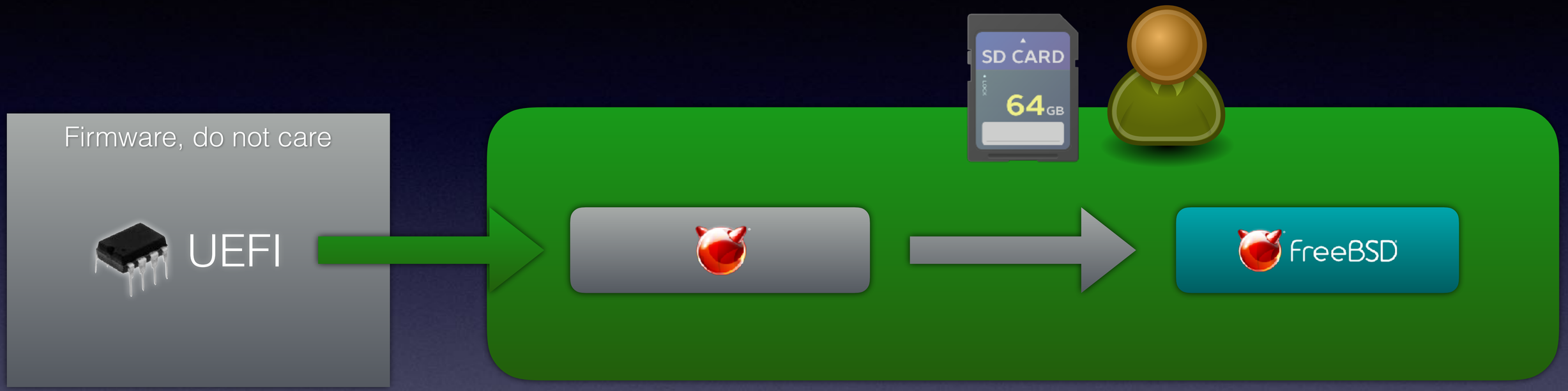
SLES 12-SP3

Advanced options for SLES 12-SP3

Start bootloader from a read-only snapshot

The highlighted entry will be executed automatically in 8s.

UEFI boot flow advantages



UEFI boot flow advantages

tianocore

U-Boot

tianocore

```
EFI_STATUS
EFIAPI
GetNextMonotonicCount (
  OUT UINT64  *Count
  )
{
  if (Count == NULL) {
    return EFI_INVALID_PARAMETER;
  }

  *Count = gCurrentMonotonicCount++;
  return EFI_SUCCESS;
}
```

tianocore

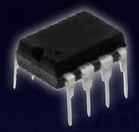
U-Boot

```
static efi_status_t EFIAPI efi_get_next_monotonic_count(uint64_t *count)
{
        static uint64_t mono = 0;
        EFI_ENTRY("%p", count);
        *count = mono++;
        return EFI_EXIT(EFI_SUCCESS);
}
```

tianocore


Lorem ipsum
dolor sit amet,
consectetuer
adipiscing elit.
Donec aliquet
diam ut enim
Lorem ipsum
dolor sit amet,
consectetuer
adipiscing elit.
Donec aliquet
diam ut enim

tianocore

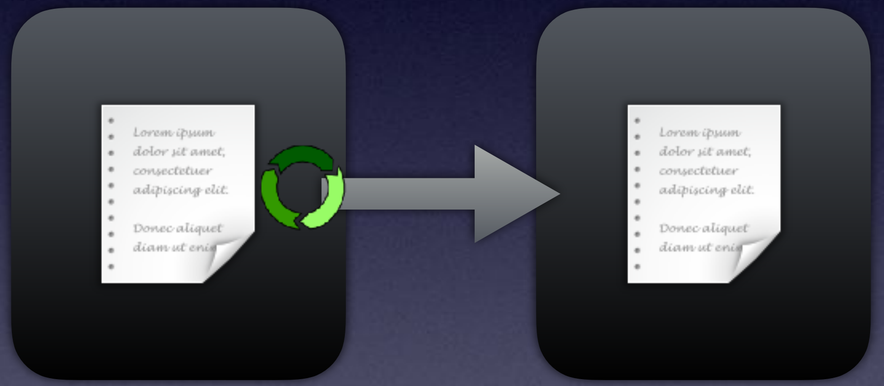


UEFI

tianocore


Lorem ipsum
dolor sit amet,
consectetuer
adipiscing elit.
Donec aliquet
diam ut enim
Lorem ipsum
dolor sit amet,
consectetuer
adipiscing elit.
Donec aliquet
diam ut enim

tianocore



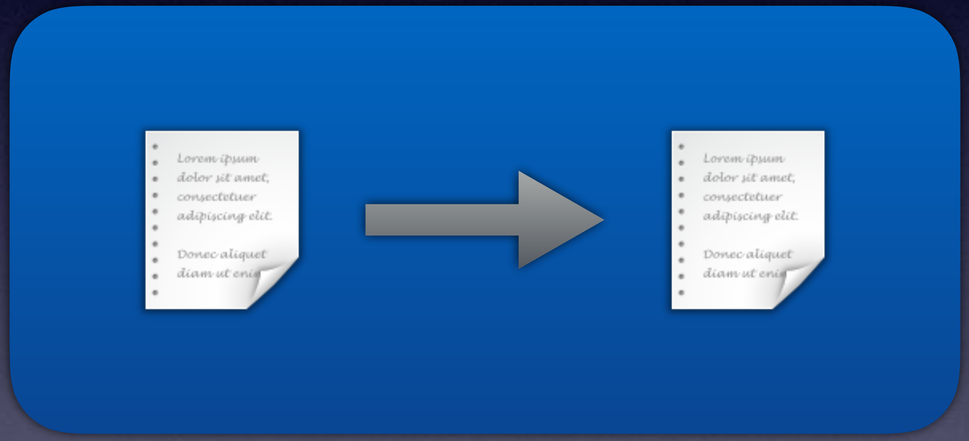
Black Boxes

tianocore

U-Boot

tianocore

U-Boot



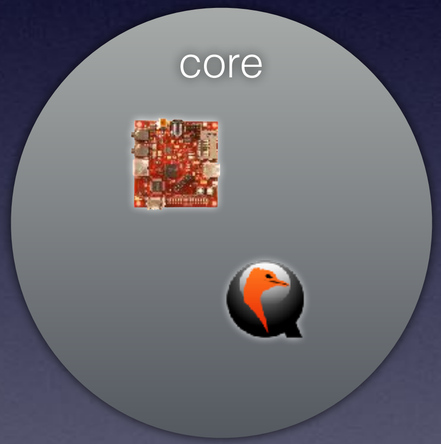
Monolithic

tianocore

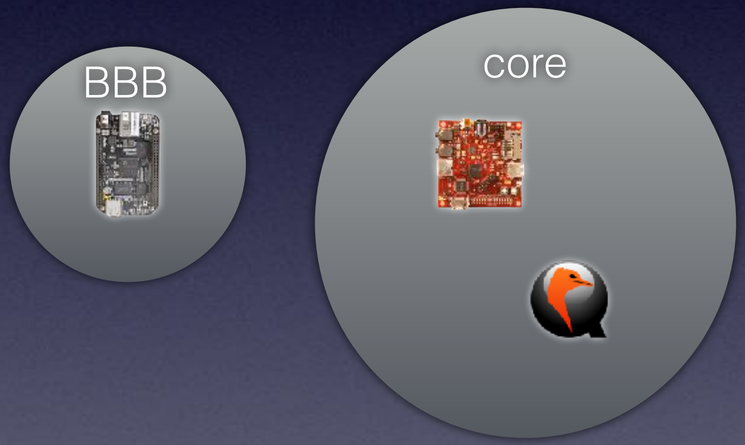
U-Boot

tianocore

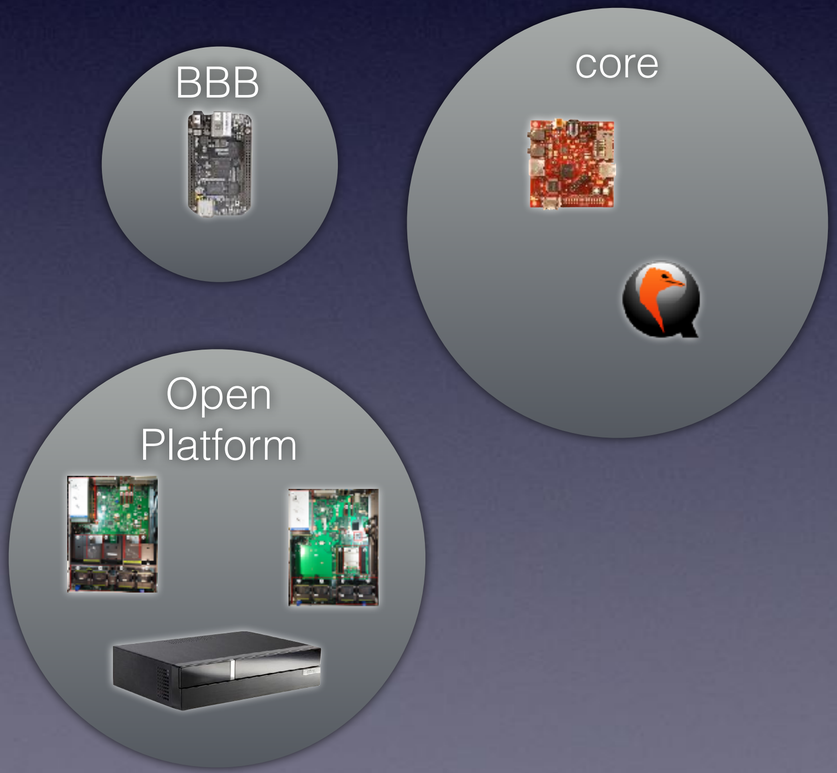
U-Boot



tianocore



tianocore



tianocore

BBB

core

Open Platform

U-Boot

$ grep -R ARM configs/ | wc -l

684

tianocore

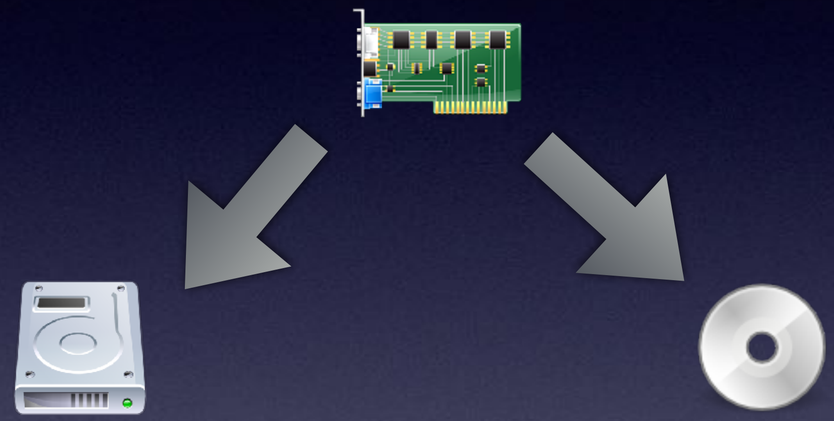
U-Boot

Foundation for black box modules	Monolithic, GPL
Windows coding style	Linux coding style
Built to fork	Built to include

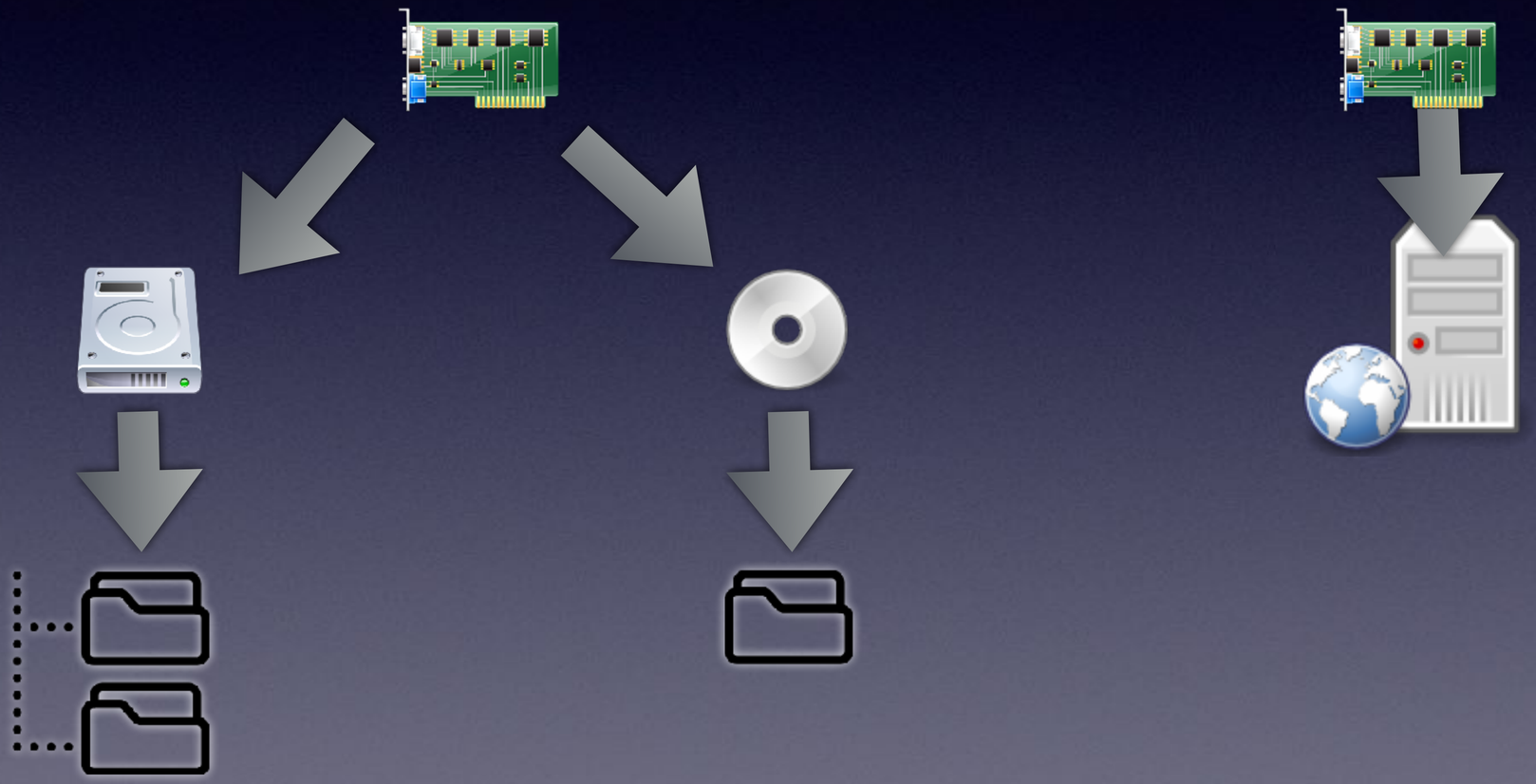
UEFI interfaces

UEFI interfaces

UEFI interfaces



UEFI interfaces

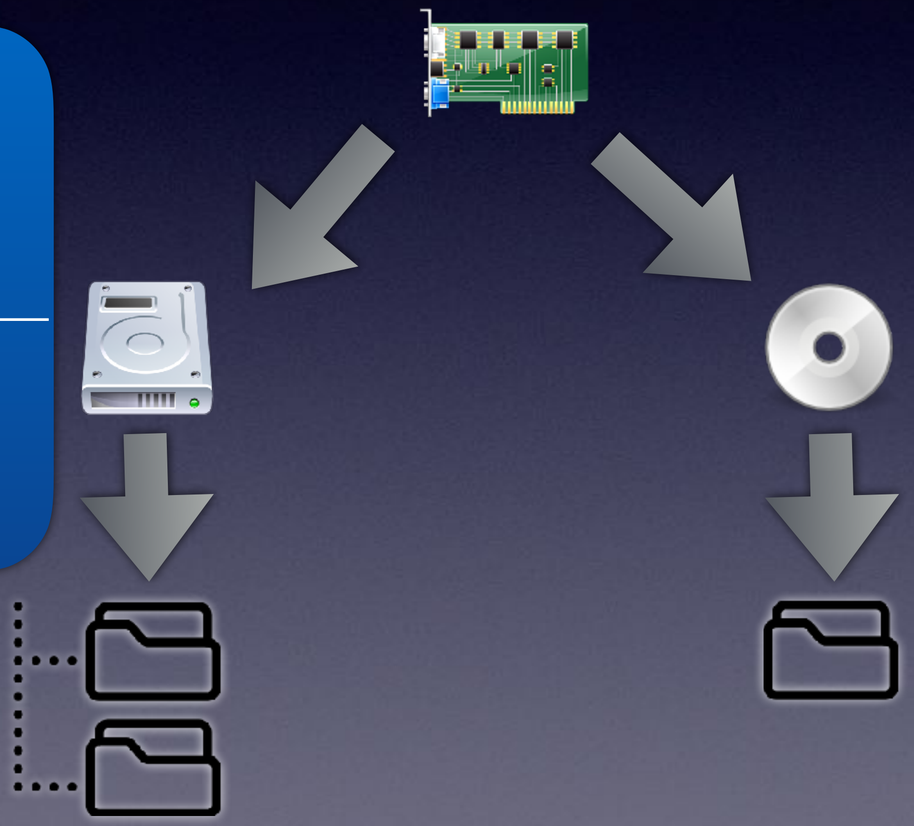


UEFI interfaces

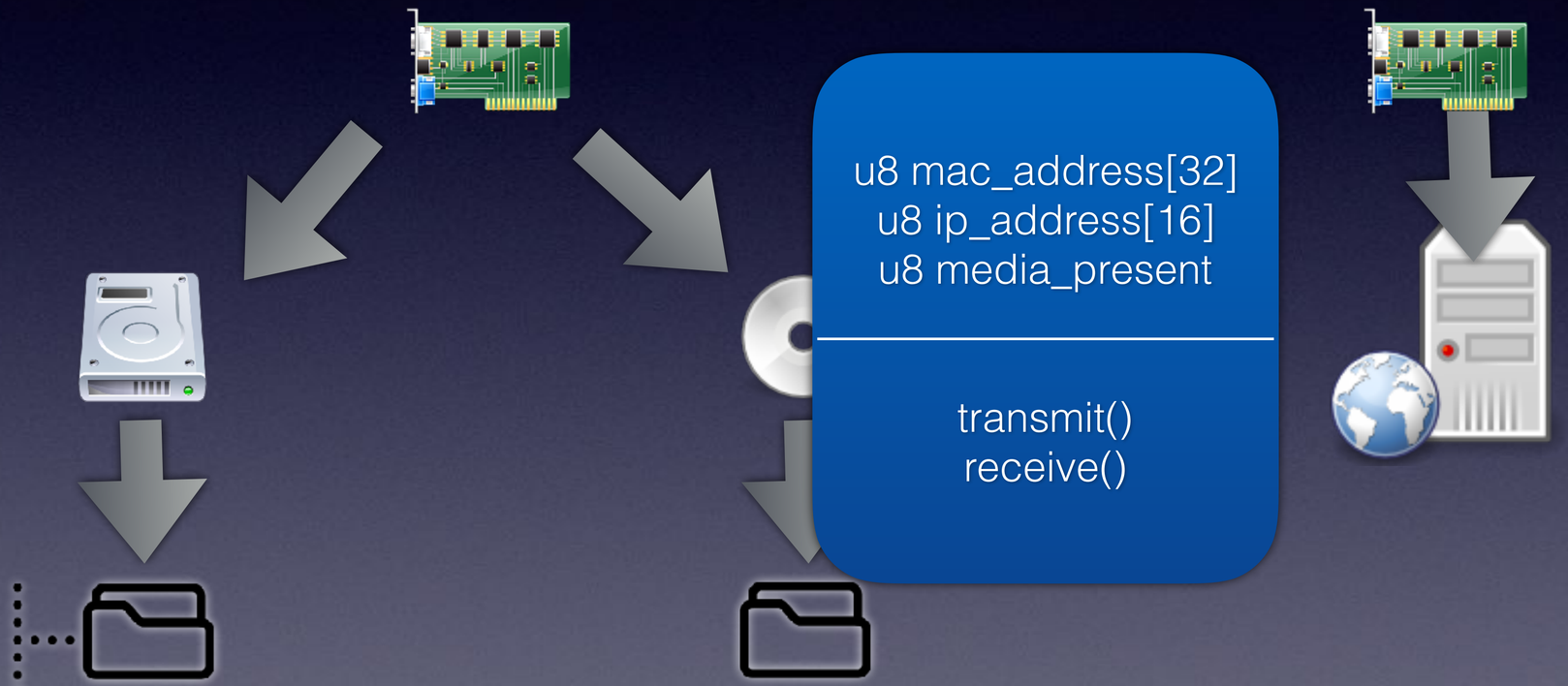
u32 block_size
u64 last_block
char read_only

---

read_blocks()
write_blocks()



UEFI interfaces



U-Boot interfaces

U-Boot interfaces

ulong blksz
u64 lba
char removable

---

blk_dread()
blk_dwrite()

---

eth_get_ethaddr()
net_send_packet()
eth_rx()

UEFI interfaces

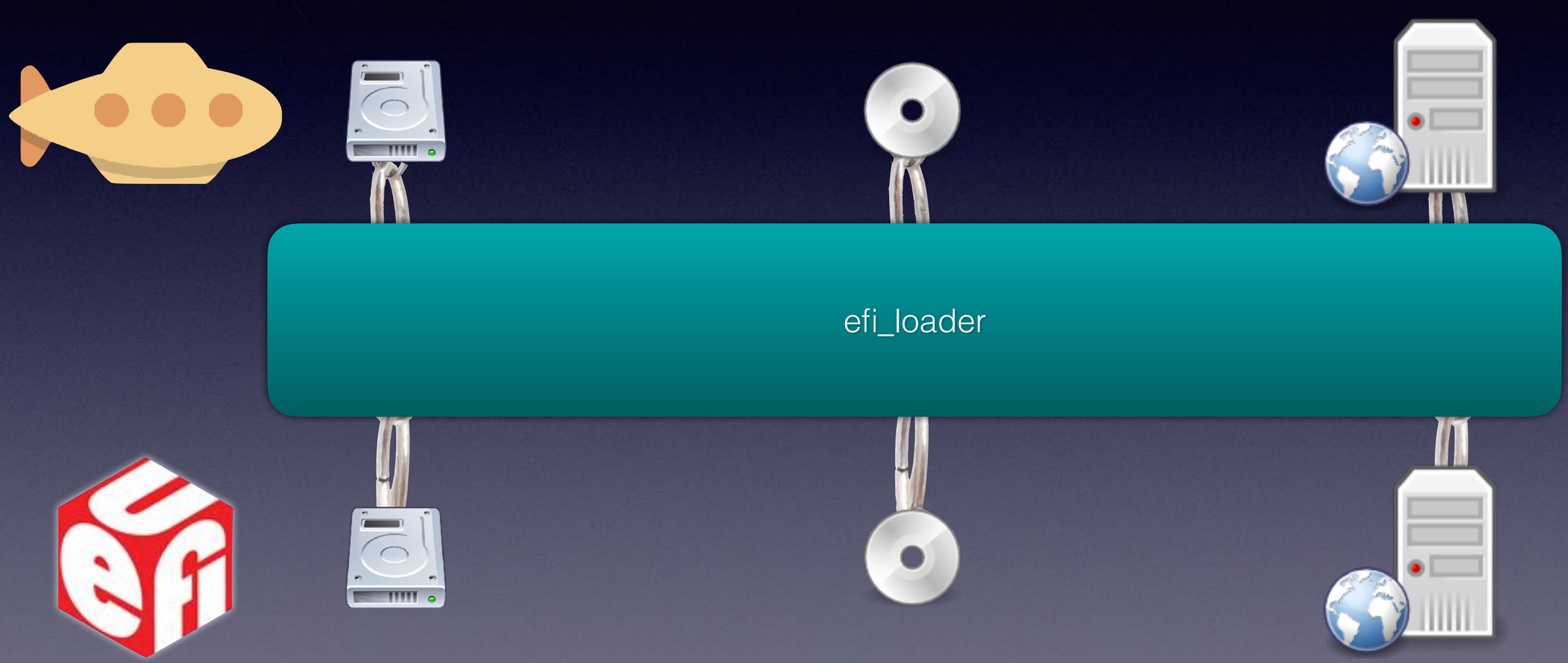







UEFI interfaces

UEFI interfaces



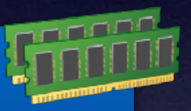
efi_loader

efi_loader

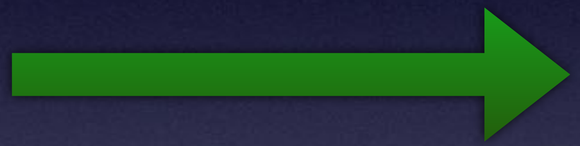
bootefi

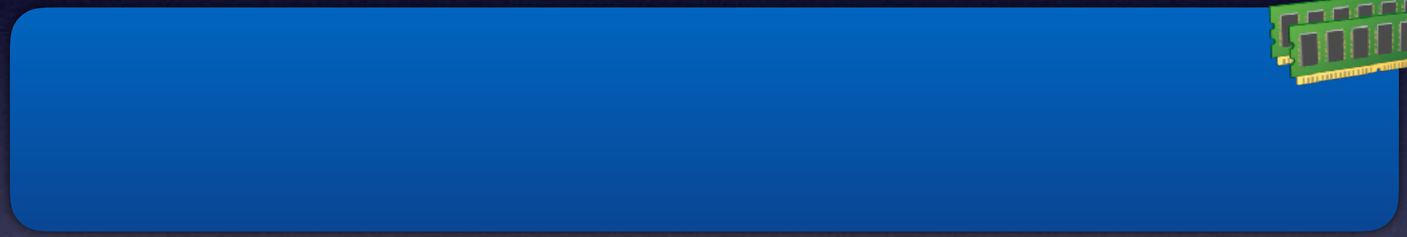
bootefi

bootefi

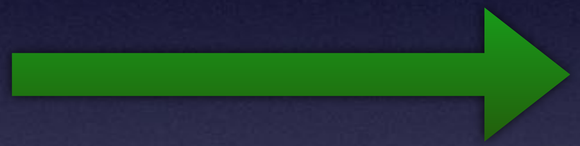


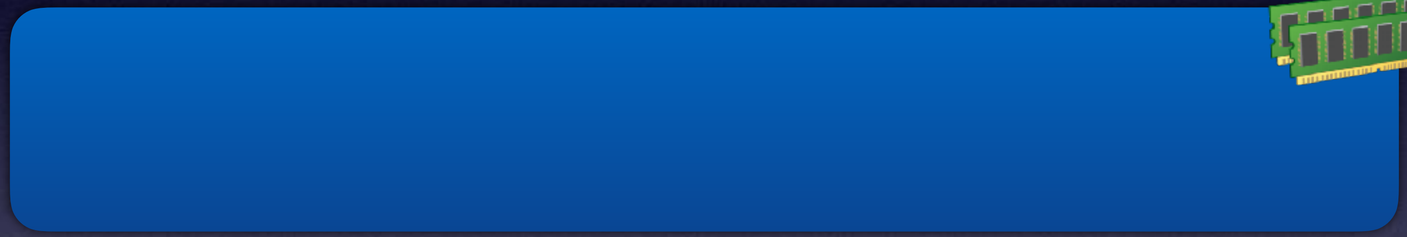
bootefi





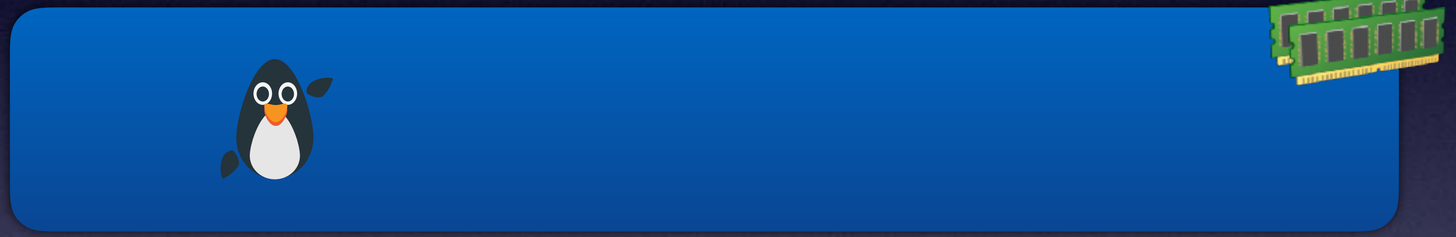
bootefi





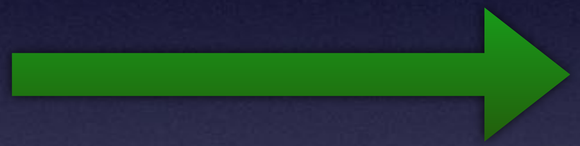

```
U-Boot> load mmc 0:1 $kernel_addr_r Image
```

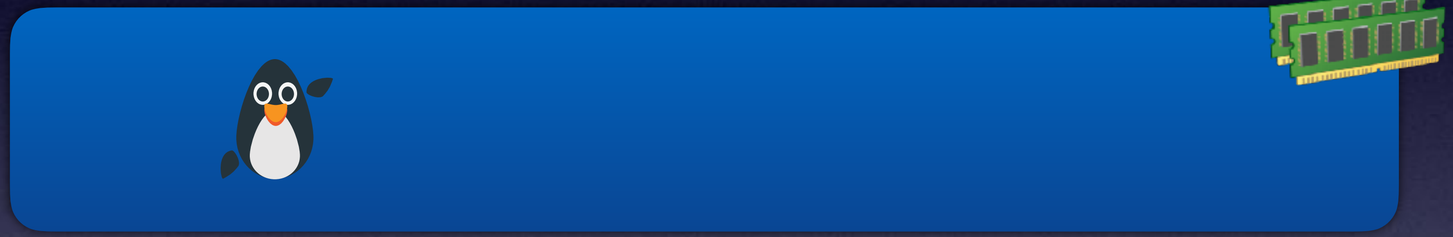
bootefi



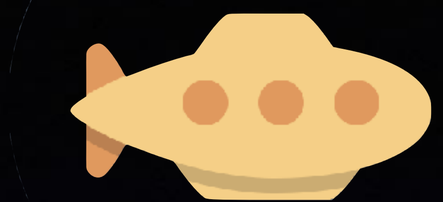
```
U-Boot> load mmc 0:1 $kernel_addr_r Image
reading Image
568320 bytes read in 165 ms (3.3 MiB/s)
```

bootefi



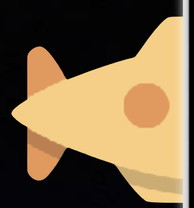


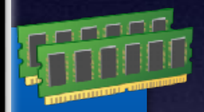
```
U-Boot> bootefi $kernel_addr_r $fdt_addr_r
```



bootefi

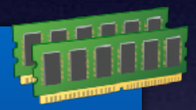
```
U-Boot> bootefi $kernel_addr_r $fdt_addr_r
## Starting EFI application at 0x01000000 …
EFI stub: Booting Linux Kernel...
EFI stub: UEFI Secure Boot is enabled.
EFI stub: Using DTB from configuration table
EFI stub: Exiting boot services and installing virtual
address map...
```



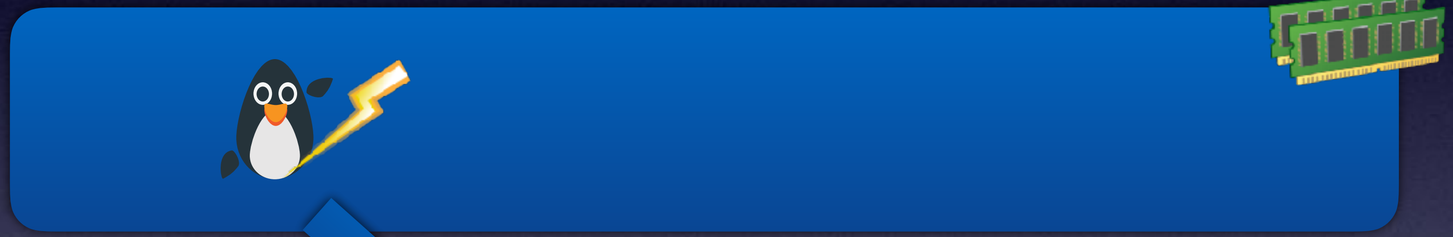


virtua

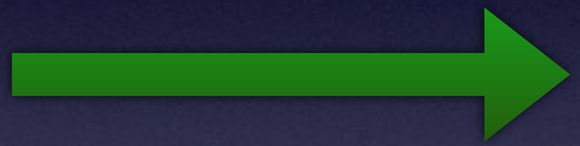
bootefi



bootefi



bootefi



KASLR

efi_loader

bootefi

efi_loader

bootefi

distro boot

distro boot

distro boot

boot_targets=mmc0 usb0 pxe dhcp

distro boot

boot_targets=mmc0 usb0 pxe dhcp

extlinux

distro boot

boot_targets=mmc0 usb0 pxe dhcp

extlinux

boot.script

distro boot

boot_targets=mmc0 usb0 pxe dhcp

extlinux

boot.script

EFI

distro boot

EFI

distro boot

EFI

distro boot

EFI

ESP

Partition Table

distro boot

EFI

ESP

$fdtfile

distro boot

EFI

ESP

/

/dtb/

/dtb/current/

/boot/

/boot/dtb/

/boot/dtb/current/

$fdtfile

distro boot

EFI

ESP

$fdtfile

efi/boot/bootaa64.efi

distro boot

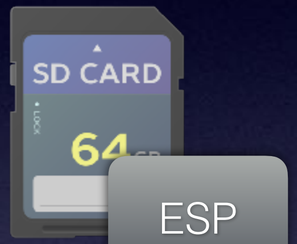
EFI

ESP

$fdtfile

distro boot

EFI



ESP

$fdtfile


SD CARD
64

distro boot

EFI

distro boot

EFI

distro boot

EFI

distro boot

EFI

el torito

ISO9660

distro boot

EFI

el torito

ISO9660

el torito

distro boot

EFI

el torito

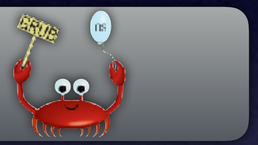
Partition Table

el torito

distro boot

EFI

$fdtfile



el torito

Partition Table

el torito

distro boot

EFI

distro boot

EFI

DHCP Distro Boot

distro boot

EFI

DHCP Distro Boot

DHCP Server

distro boot

EFI

DHCP req

DHCP Distro Boot

DHCP Server

distro boot

EFI

EFI & Arch VCI

DHCP req

DHCP Distro Boot

DHCP Server

distro boot

EFI

DHCP Distro Boot

EFI & Arch VCI

DHCP req

filename

DHCP ack

DHCP Server

distro boot

EFI

DHCP Distro Boot

EFI & Arch VCI

DHCP req

filename

DHCP ack

DHCP Server

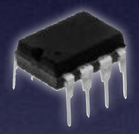
TFTP

distro boot

EFI

UEFI Tables

UEFI Tables



UEFI

bootaa64.efi

EFI Runtime Data

Console
Boot Services
Runtime Services
Tables

UEFI Tables

UEFI Tables

Tables

devicetree
.org

ACPI

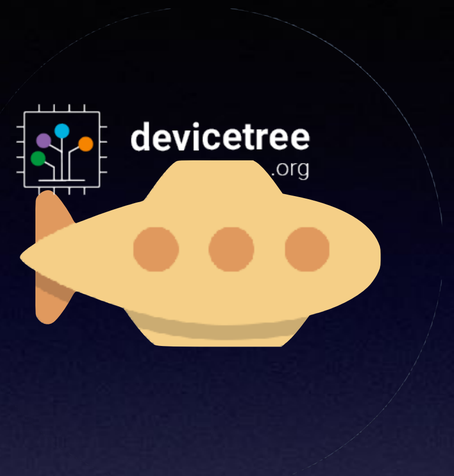
UEFI Tables

Tables

devicetree
.org

~~ACPI~~

UEFI Tables

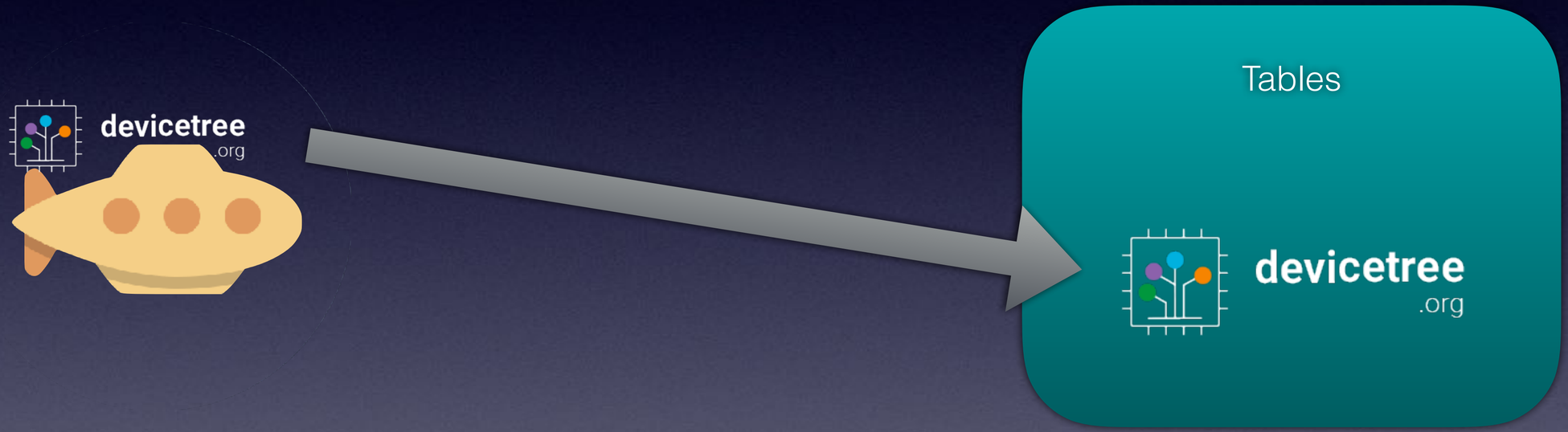


Tables

devicetree
.org

~~ACPI~~

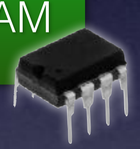
UEFI Tables



Missing Features

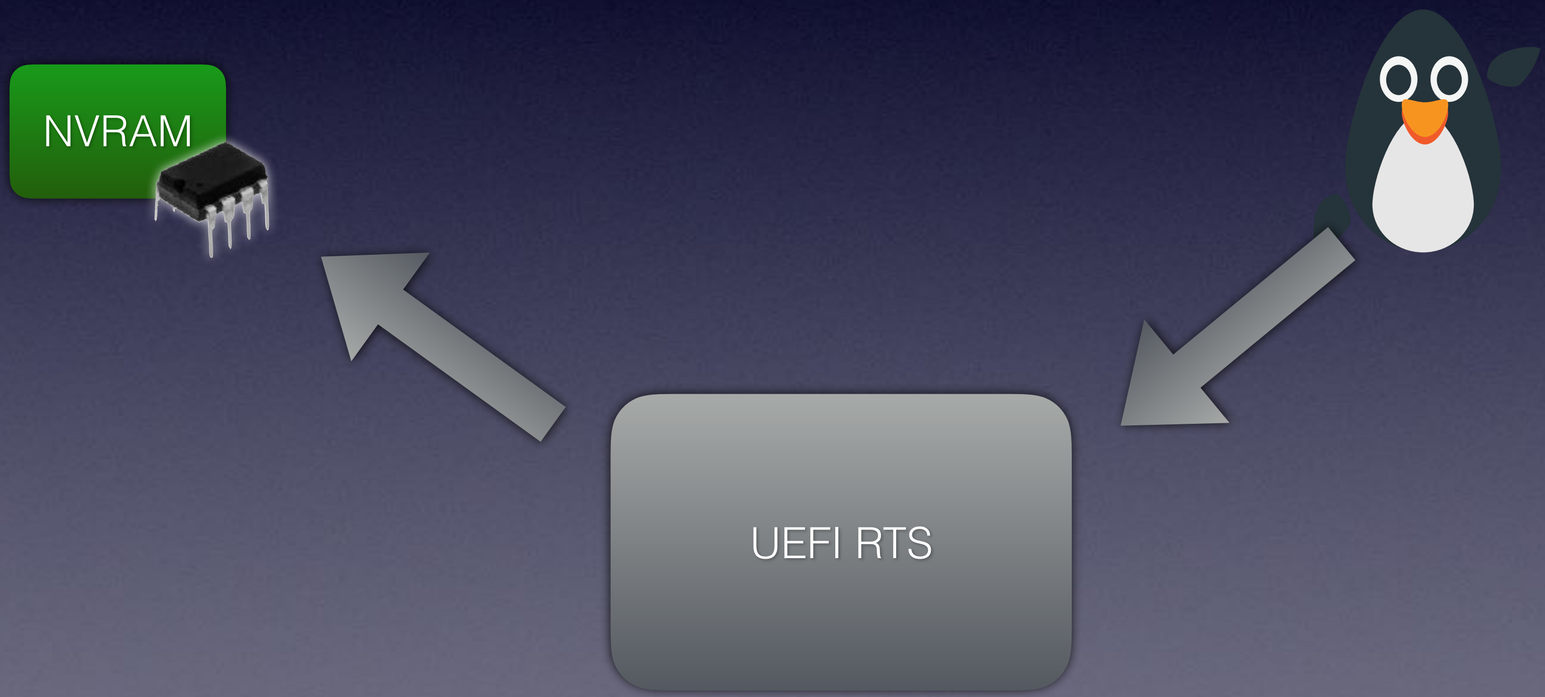
Missing Features

NVRAM



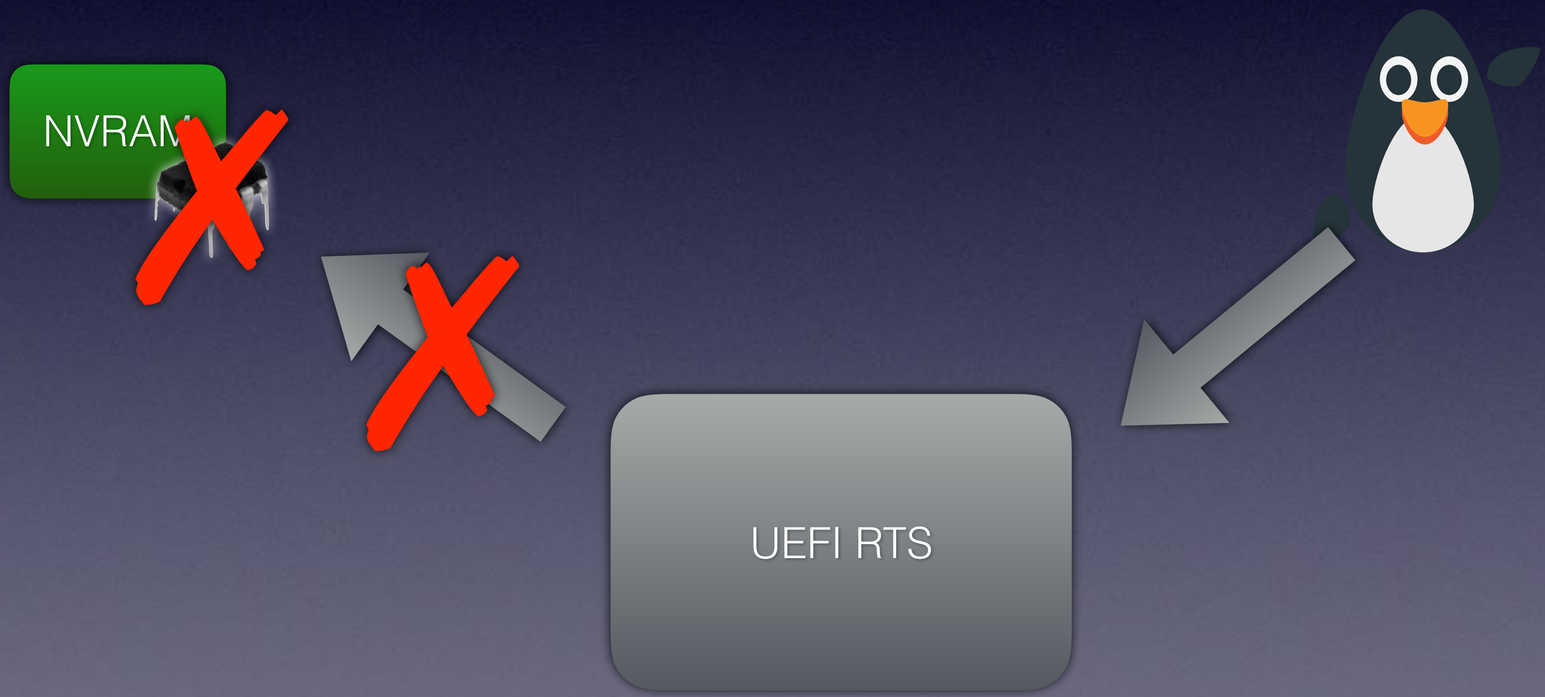
Missing Features

Missing Features



Missing Features

Missing Features



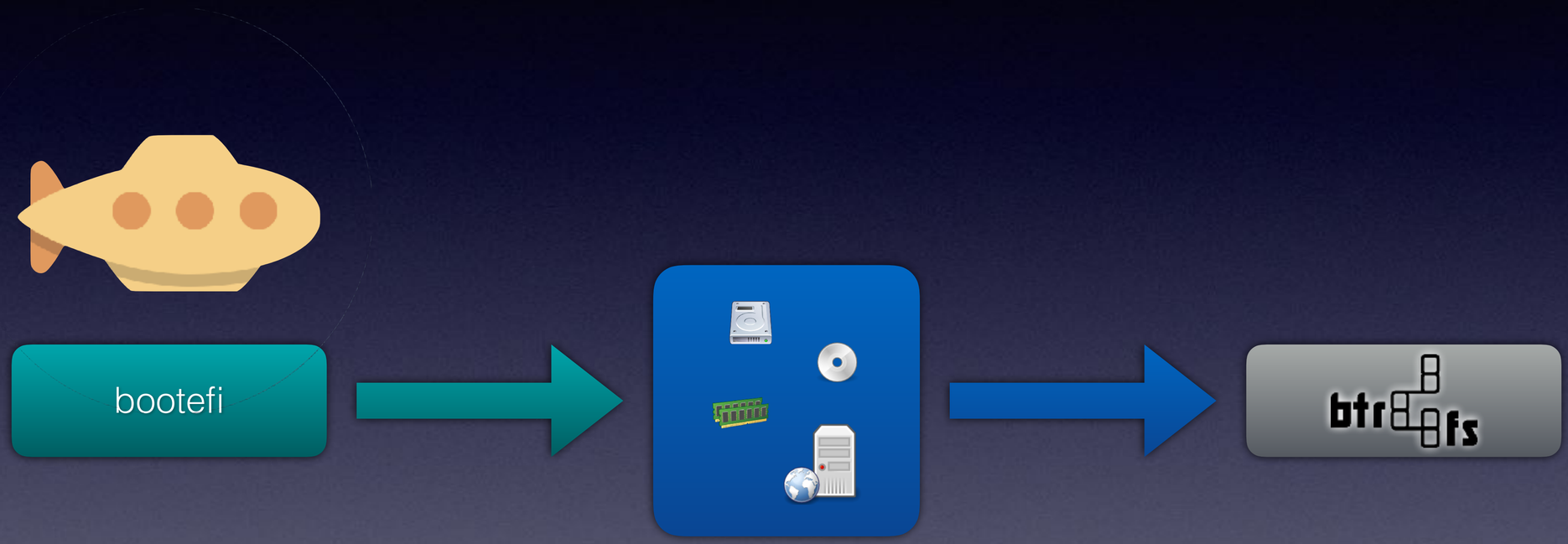
Missing Features

Missing Features

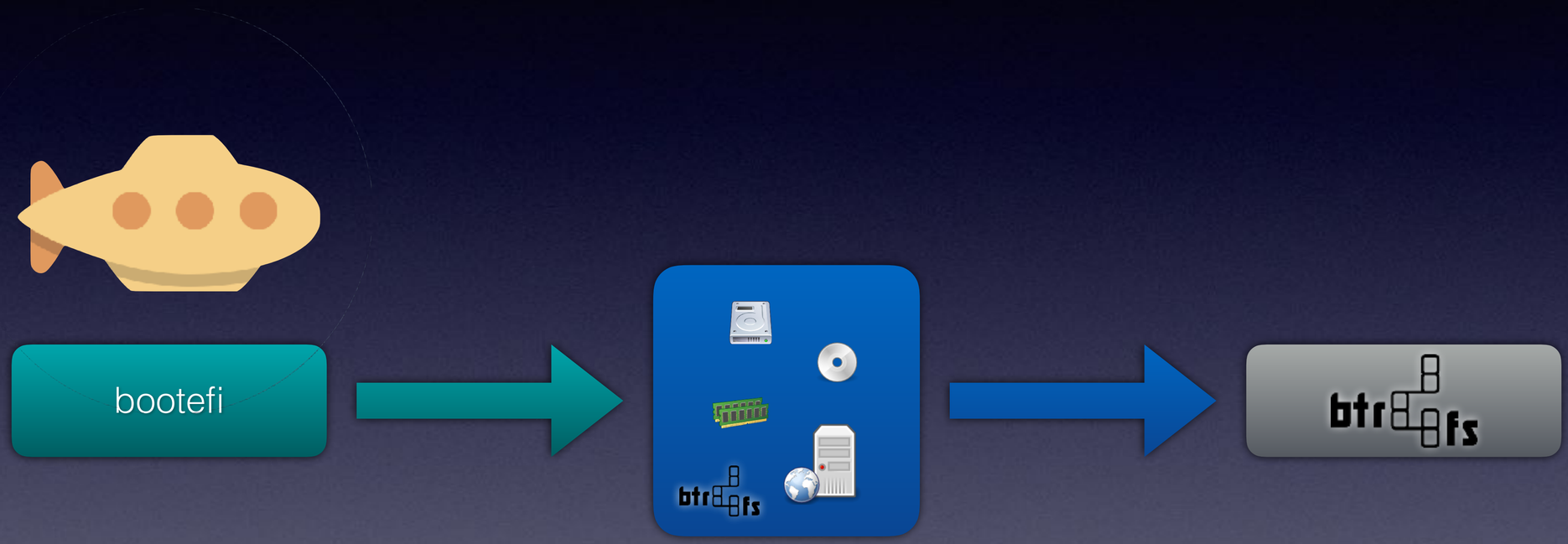
Missing Features

Missing Features

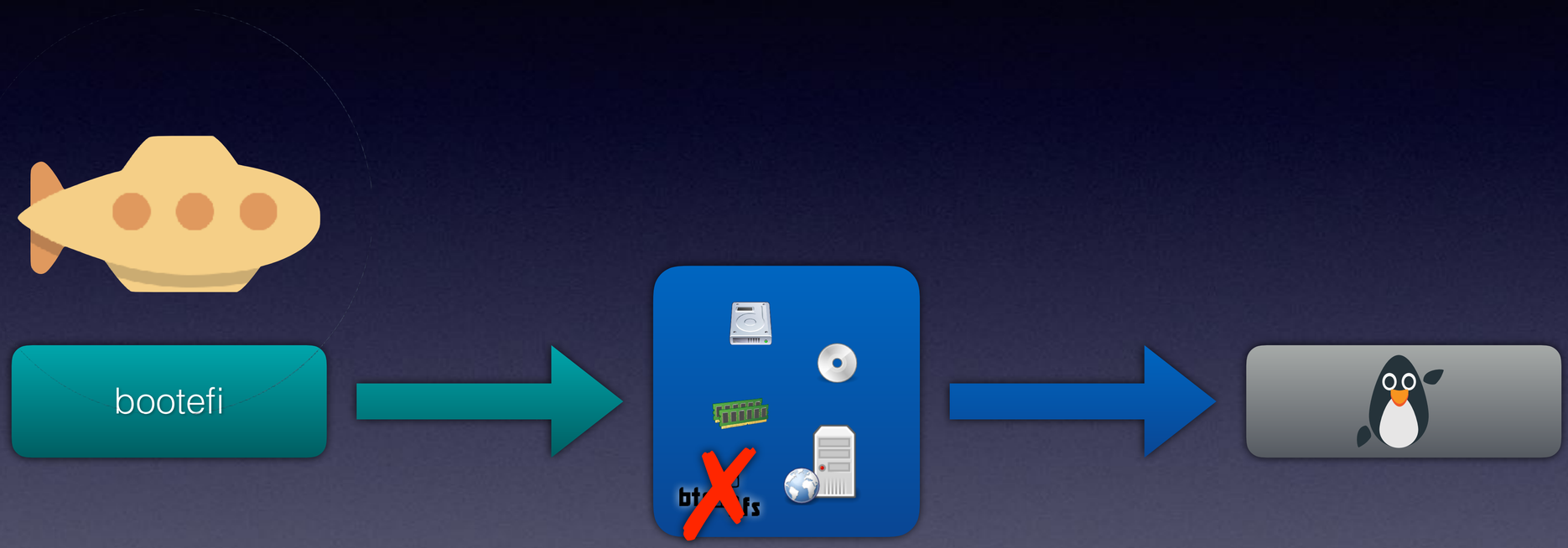
Missing Features



Missing Features



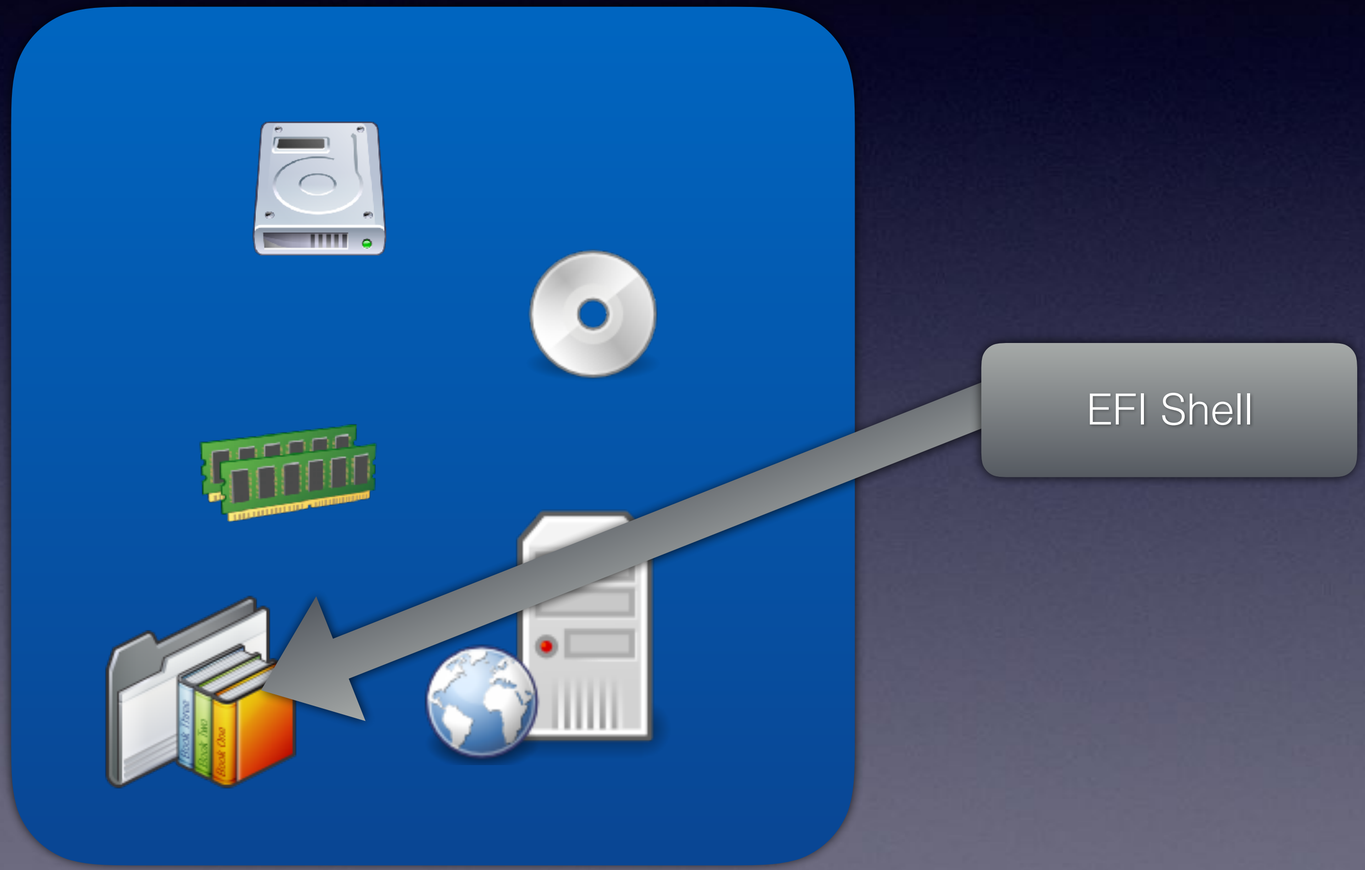
Missing Features



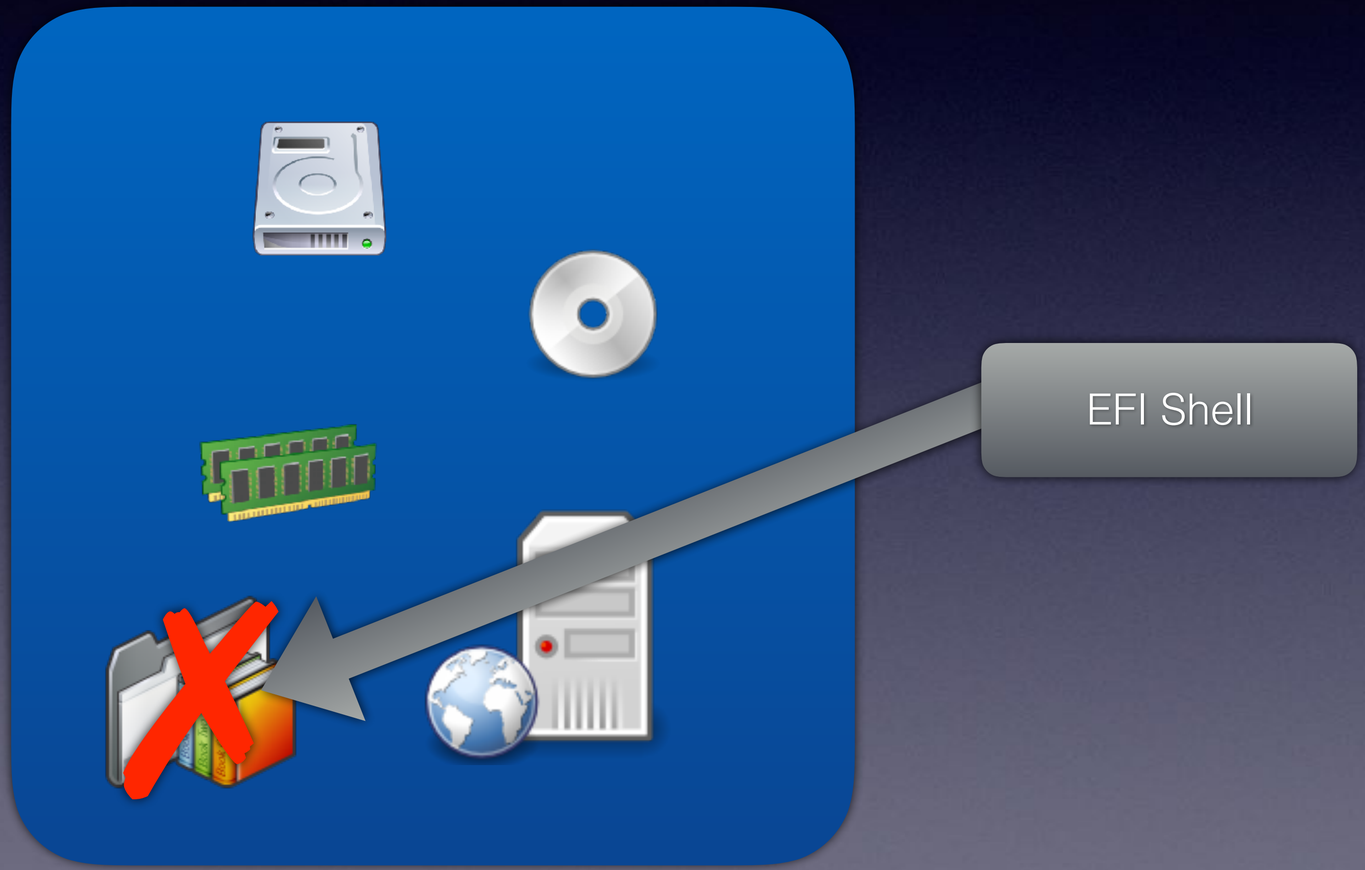
Missing Features

Missing Features

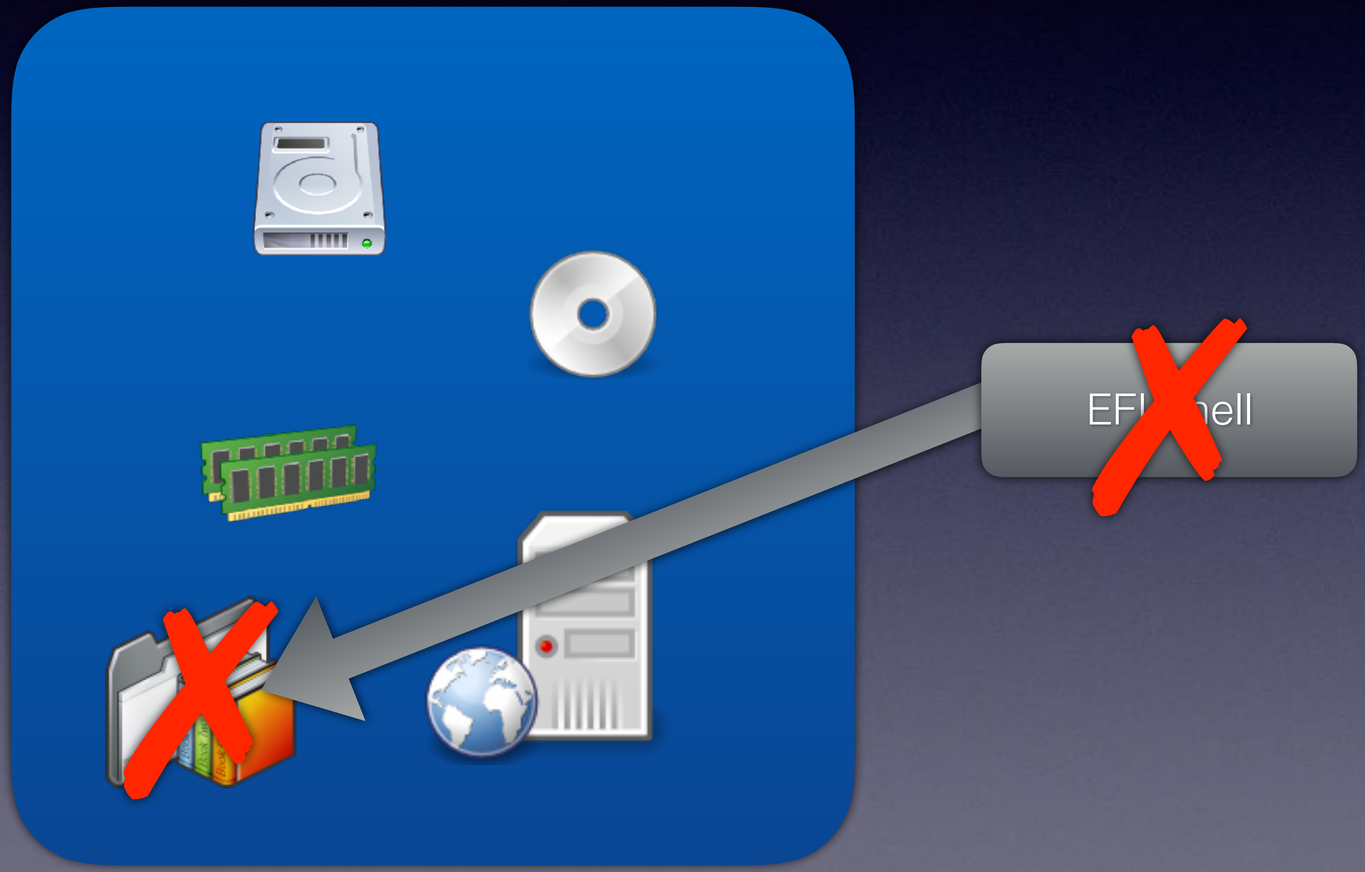
Missing Features



Missing Features

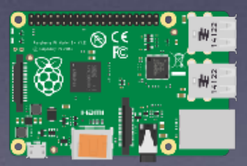


Missing Features



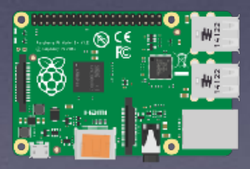
Why?

Why?



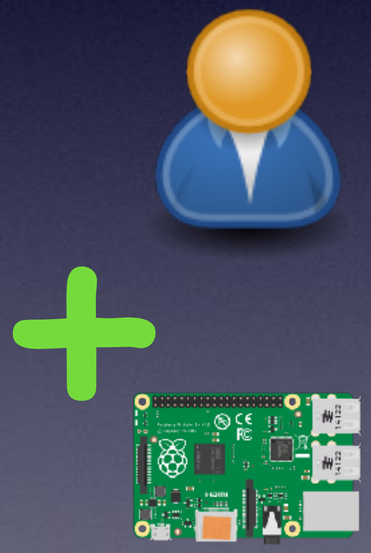
Why?

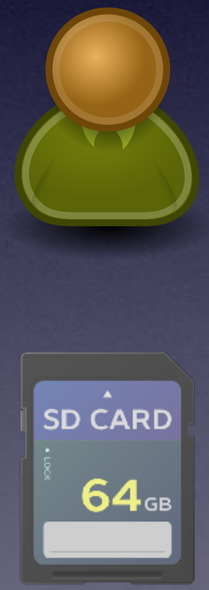
Department A



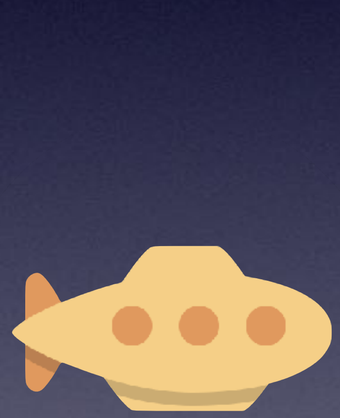
Department B

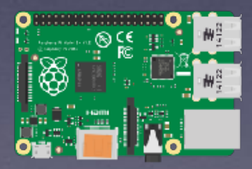
Why?



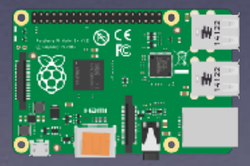


Why?

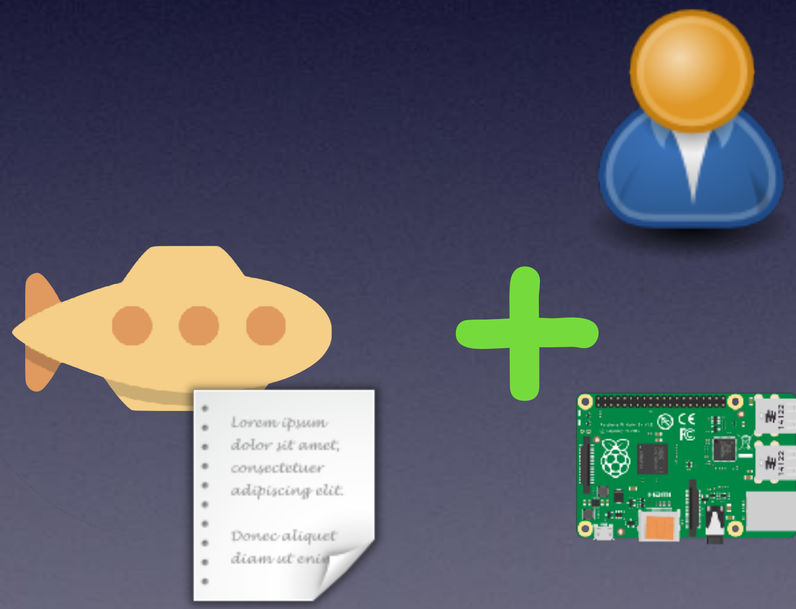




Why?

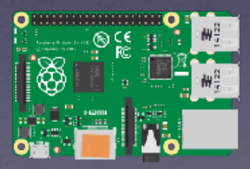


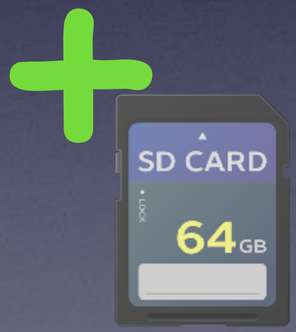
Why?


Lorem ipsum
dolor sit amet,
consectetuer
adipiscing elit.
Donec aliquet

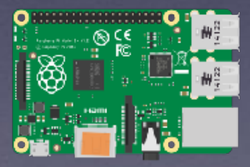

SD CARD
64GB

Why?

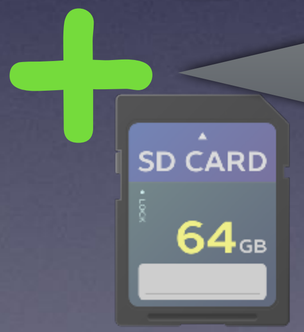




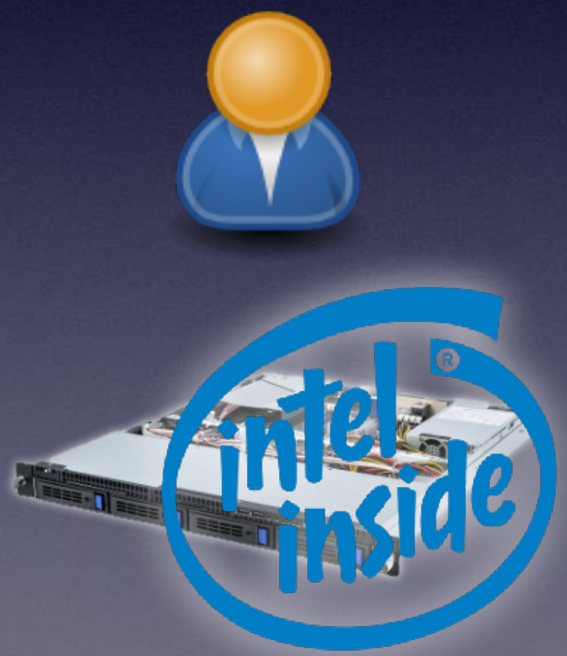
Why?

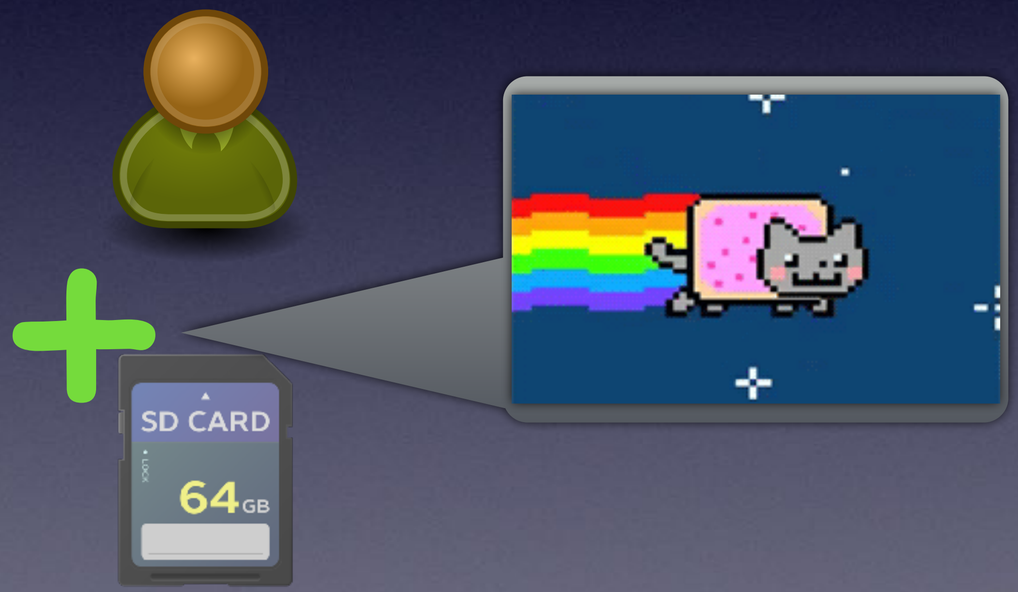


Why?



Why?





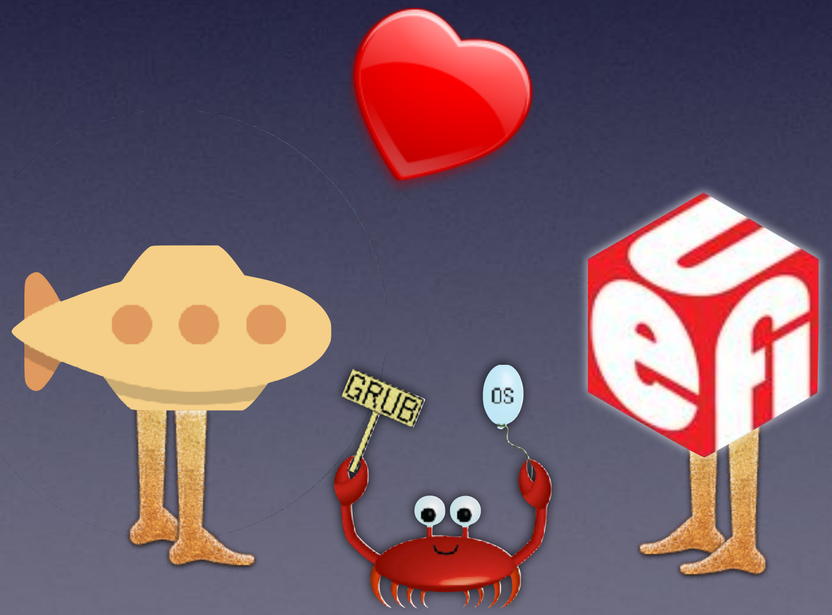
Why?

Why?

FreeBSD

Why?

Thank You



Further Information

https://events.opensuse.org/conference/oSC16/program/proposal/946

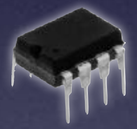
External Sources

https://commons.wikimedia.org/wiki/File:Raspberry_Pi_B%2B_illustration.svg

https://commons.wikimedia.org/wiki/File:Sd-card-1377140.svg

http://eu.mophie.com/shop/media/catalog/product/cache/3/small_image/270x330/9df78eab33525d08d6e5fb8d27136e95/u/s/usb-micro3-40-blk_usb-tip-detail_front-back_540px.jpg

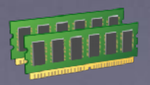
https://commons.wikimedia.org/wiki/File:Circle-icons-submarine.svg



https://commons.wikimedia.org/wiki/File:150-8-DIP.jpg

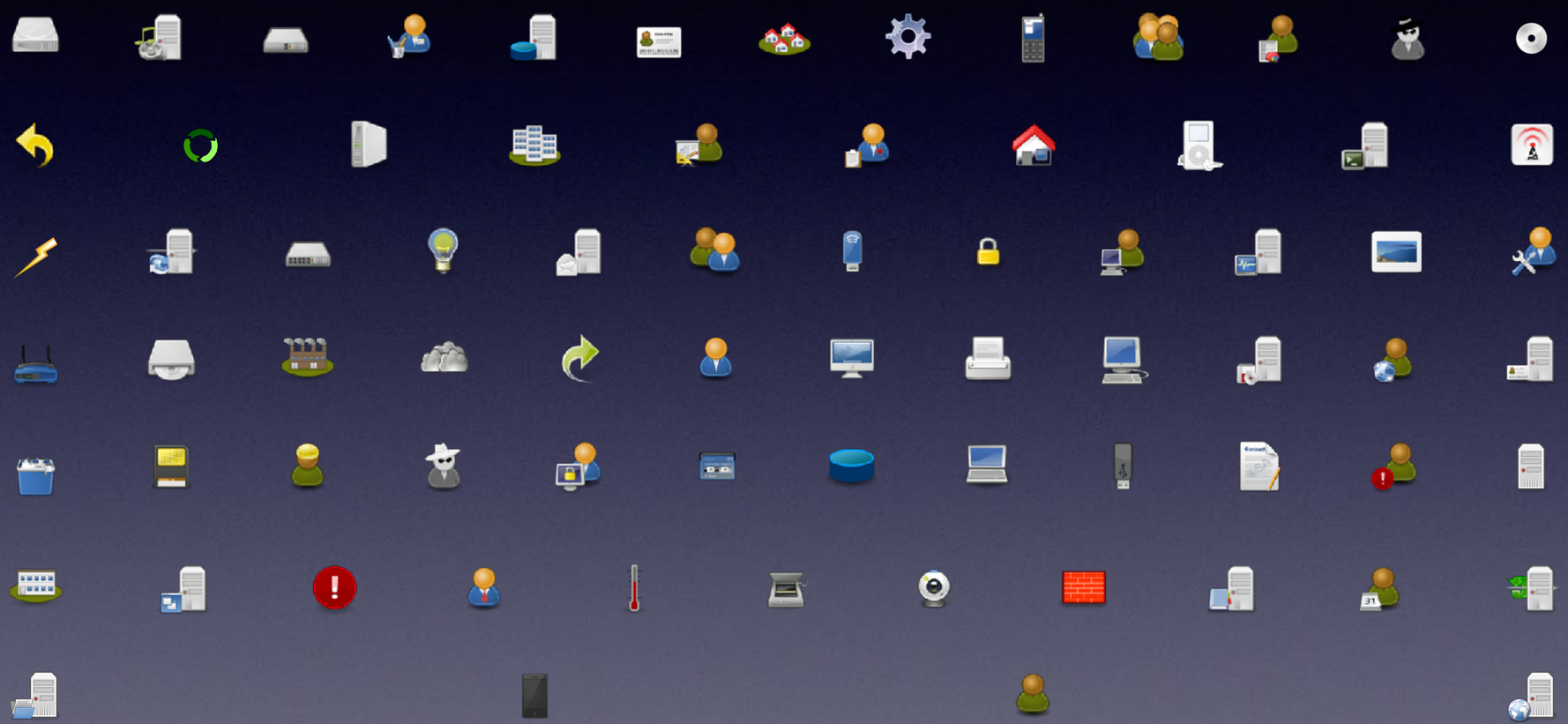
https://commons.wikimedia.org/wiki/File:Hdd_icon.svg

https://commons.wikimedia.org/wiki/File:ARM_CPU_icon.svg



http://findicons.com/icon/177982/memory#

OSA Icons



Icons received from http://www.opensecurityarchitecture.org/cms/library/icon-library

emojione Icons



Icons received from http://www.opensecurityarchitecture.org/cms/library/icon-library

Other Icons

http://findicons.com/icon/202613/folder_library

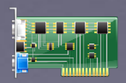
http://findicons.com/icon/download/234261/clock/128/png

http://findicons.com/icon/439269/button_power

https://fosdem.org/2017/schedule/event/grub_new_maintainers/attachments/slides/1768/export/events/attachments/grub_new_maintainers/slides/1768/slides.pdf

https://de.wikipedia.org/wiki/BeagleBoard#/media/File:Beagle_Board_big.jpg

https://thenounproject.com/term/folder-tree/27307/



https://commons.wikimedia.org/wiki/File:Crystal_Project_Hardware.png

Other Icons

http://tumboy.tumblr.com/post/10052361836

http://findicons.com/icon/132807/b_leg_embossed

http://findicons.com/icon/237892/text_plain

http://findicons.com/icon/226957/package_games_board